9

ON TWO CONGRUENCES FOR PRIMALITY

M. V. SUBBARAO

Reprinted from Pacific Journal of Mathematics Vol. 52, No. 1
1 9 7 4

PACIFIC JOURNAL OF MATHEMATICS
Vol. 52, No. 1, 1974

ON TWO CONGRUENCES FOR PRIMALITY

M. V. SUBBARAO

In this paper we consider the congruences

$$n\sigma(n) \equiv 2(\text{mod}\ \varphi(n))\ , \quad \varphi(n)t(n) + 2 \equiv 0\ (\text{mod}\ n)\ .$$

1. Introduction. Apart from the classical Wilson's theorem (that a positive integer $p > 1$ is a prime if and only if $(p-1)! + 1 \equiv 0\ (\text{mod}\ p)$) and its variants and corollaries, there is probably no other simple primality criterion in the literature in the form of a congruence. In this connection, we may recall Lehmer's congruence [1]:

$$n - 1 \equiv 0\ \text{mod}\phi(n)\ . \tag{1.1}$$

This is satisfied by every prime. We do not yet know if it has any composite n as a solution. In 1932, Lehmer [1] showed that if there exists a composite number n satisfying (1.1), then n must be odd and square free and have at least seven distinct prime factors. This result was improved in 1944 by Fr. Schuh [4] who showed that such a n must have at least eleven prime factors. In 1970, E. Lieuwens [2] corrected an error in the proof of Schuh.

In the congruences we shall consider,

$$n\sigma(n) \equiv 2(\text{mod}\ \phi(n)) \tag{1.2}$$

and

$$\phi(n)t(n) + 2 \equiv 0(\text{mod}\ n)\ , \tag{1.3}$$

where $\phi(n)$ is Euler's totient, and $t(n)$ and $\sigma(n)$ are respectively the number and sum of the divisors of n. Each of these is satisfied whenever n is a prime. It is a simple matter to solve (1.2) completely (Theorem 1). However, the problem of solving (1.3) for all composite integers n seems to be a deep one, and we offer only a partial solution.

2. THEOREM 1. *The only composite numbers n satisfying* (1.2) *are* $n = 4$, 6, *and* 22.

Proof. Let a solution of (1.2) be

$$n = 2^a p_1^{a_1} \cdots p_r^{a_r}$$

where $p_1, \cdots, p_r$ are the distinct odd prime divisors of n. If for some $i(1 \leqq i \leqq r)$, $a_i > 1$, then $p_i \mid \phi(n)$ and $p_i \mid n$, so that $p_i \mid 2$, an absurdity. Hence

$$a_1 = a_2 = \cdots = a_r = 1 .$$

An analogous argument shows that $a = 0, 1$ or 2. Hence $n = 2^a p_1 p_2 \cdots p_r$, where $a = 0, 1$ or 2. Next, when n is in this form, $2^r \mid \sigma(n)$ and $2^r \mid \phi(n)$, so that we should have $2^r \mid 2$, on using the congruence. Hence $r = 0$ or 1, and we get $n = 2, 4, p_1, 2p_1, 4p_1$ for the possible solutions of (1.2). However, $n = 4p_1$ is impossible, for otherwise $4 \mid \phi(n)$, and this would imply, on using the congruence, that $4 \mid 2$.

In the next place, if $n = 2p_1$, we have

$$6p_1(p_1 + 1) \equiv 2 \bmod (p_1 - 1) .$$

This shows that $(p_1 - 1) \mid 10$, and this gives $p_1 = 2, 3$, and 11. Hence all the possible composite solutions of (1.2) are $n = 4, 6$, and 22, and these are indeed solutions of the congruence.

3. **The solution of congruence (1.3).** Up to 100,000, the only composite solution of (1.3) is $n = 4$, and the question naturally arises if there is any composite solution > 4. While this is still open, we devote the rest of the paper to obtain some information about such a solution if it exists.

THEOREM 2. *Every composite solution $n > 4$ of the congruence* (1.3) *satisfies the following conditions:*

(A) *n is square-free.*

(B) *If p is an odd prime divisor of n, then there is no prime divisor of the form $px + 1$.*

(C) *Let K be defined by the relation*

$$\phi(n)t(n) + 2 = Kn . \tag{3.1}$$

Then K and n are of opposite parity and $4 \nmid K$.

(D) *If $n = m$ is a solution of* (1.3), *then $n = 2m$ is not a solution.*

Proof. For an odd prime p, if $p^2 \mid n$, then $p \mid \phi(n)$; hence on using (1.2), $p \mid 2$, which is absurd. Again if $4 \mid n$ and $n > 4$, a simple argument shows that (1.3) is impossible. This establishes result (A). The proofs of (B), (C), and (D) are equally easy.

LEMMA. *For a given r, the number of solutions n of* (2.11) *having r prime divisors is finite. In fact, if $p_1, p_2, \cdots, p_r$ are the prime divisors of n in increasing order of magnitude, and if*

$$Q_r = \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) \cdots \left(1 - \frac{1}{q_r}\right) \tag{3.2}$$

where q_r *is the* rth *prime in the sequence of primes* 2, 3, 5, $\cdots$ ($q_1 = 2$, $q_2 = 3$ etc.), *then*

$$2^r Q_r \leqq K \leqq 2^r , \tag{3.3}$$

$$p_1 < r\left(1 - \frac{K}{2^r}\right)^{-1} , \tag{3.4}$$

and for $i = 2, 3, \cdots, r$,

$$p_{i-1} < p_i < (r - i + 1)\left(1 - \frac{K}{2^r} - \frac{1}{p_1} - \cdots - \frac{1}{p_{i-1}}\right)^{-1} .$$

Proof. The relation (3.1) gives

$$\begin{aligned} K &= \frac{\phi(n)t(n)}{n} + \frac{2}{n} \\ &\leqq t(n) + \frac{2}{n} , \end{aligned}$$

for $n > 2$. Hence $K \leqq t(n)$. Since by Theorem 2, n is square free, $n = p_1, p_2, \cdots, p_r$, so that $t(n) = 2^r$. Hence $K \leqq 2^r$.

In the next place,

$$\begin{aligned} K &> 2^r \frac{\phi(n)}{n} \\ &= 2^r \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \geqq 2^r Q_r . \end{aligned}$$

This completes the proof of (3.3). To prove (3.4), we note that

$$\begin{aligned} K &> 2^r \frac{\phi(n)}{n} = 2^r \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \\ &> 2^r\left(1 - \frac{1}{p_1} - \cdots - \frac{1}{p_r}\right) . \end{aligned}$$

Hence,

$$1 - \frac{K}{2^r} < \frac{1}{p_1} + \cdots + \frac{1}{p_r} < \frac{r}{p_r} ,$$

and this gives

$$p_1 < r\left(1 - \frac{K}{2^r}\right)^{-1} .$$

Again, using

$$\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_r} < \frac{1}{p_1} + \frac{r-1}{p_2}$$

and proceeding as before, we get

$$p_1 < p_2 < (r-1)\left(1 - \frac{K}{2^r} - \frac{1}{p_1}\right)^{-1}. \tag{3.5}$$

Continuing this process, we obtain

$$p_2 < p_3 < (r-2)\left(1 - \frac{K}{2^r} - \frac{1}{p_1} - \frac{1}{p_2}\right)^{-1}, \tag{3.6}$$

and finally,

$$p_{r-1} < p_r < \left(1 - \frac{K}{2^r} - \frac{1}{p_1} - \cdots - \frac{1}{p_{r-1}}\right)^{-1}. \tag{3.7}$$

This establishes (3.4).

For a given r, (3.3) shows that K can take only a finite number of values, and (3.4)–(3.7) show that $p_1, p_2, \cdots, p_r$ can take only a finite number of values. Thus for a given r, the congruence (1.3) has got only a finite number of solutions, since for a given r the upper and lower bounds for $K, p_1, p_2, \cdots, p_r$ are fixed by the relations (3.3) and (3.4). The actual solutions corresponding to any given r can be obtained after a finite number of trials. Following this method, we have obtained the following results. (The details of the numerous computations involved in the proofs of Theorems 3 and 4 below are available with the authors.)

THEOREM 3. *Any composite solution* $n > 4$ *of* (1.3) *must have at least* 4 *distinct odd prime factors.*

THEOREM 4. *For the congruence* (1.3) *we have the following*:

(3.8) *If* $K = 1$ *or* $3 \leq K \leq 14$, *there are no solutions.*
(3.9) *If* $K = 2$, *the only solutions are all the primes and* 4.
(3.10) *If* $K = 15$, *then* $r = 4$ *or* 5.
(3.11) *If* $17 \leq K \leq 29$, *then* $r = 5$.
(3.12) *If* $K = 30$ *or* 31, *then* $r = 5$ *or* 6.
(3.13) *If* $33 \leq K \leq 58$, *then* $r = 6$.
(3.14) *If* $59 \leq K \leq 63$, *then* $r = 6$ *or* 7.
(3.15) *If* $65 \leq K \leq 116$, *then* $r = 7$.
(3.16) *If* $117 \leq K \leq 127$, *then* $r = 7$ *or* 8.
(3.17) *If* $129 \leq K \leq 230$, *then* $r = 8$.
(3.18) *If* $231 \leq K \leq 255$, *then* $r = 8$ *or* 9.
(3.19) *If* $257 \leq K \leq 457$, *then* $r = 9$.
(3.20) *If* $458 \leq K \leq 551$, *then* $r = 9$ *or* 10.
(3.21) *If* $513 \leq K \leq 909$, *then* $r = 10$.
(3.22) *If* $910 \leq K \leq 1023$, *then* $r = 10$ *or* 11.

Proof. We illustrate the proof for the case when n is odd. Using the lemma, we have

$$\begin{aligned}2^r \geqq K > 2^r\Big(1-\frac{1}{p_1}\Big)\Big(1-\frac{1}{p_2}\Big)\cdots\Big(1-\frac{1}{p_r}\Big)\\ > 2^r\Big(1-\frac{1}{3}\Big)\Big(1-\frac{1}{5}\Big)\Big(1-\frac{1}{17}\Big)\Big(1-\frac{1}{23}\Big)\cdots\Big(1-\frac{1}{p_r}\Big),\end{aligned}$$

on using part (B) of Theorem 2 and Theorem 3. Giving K successive integral values and examining the consistency of the resulting inequalities while keeping in view the restrictions of Theorem 2, we get the results of the theorem.

REMARK. Any solution n of (3.1) satisfies the relation

$$2^r < \frac{6480}{19019} K e^{\gamma} \log x (1 + \log^{-2} x)$$

where γ is Euler's constant, r is the number of distinct prime factors of n and $x = q_{r+5}$. To show this, we note that

$$\begin{aligned}2^r = t(n) < K\frac{n}{\phi(n)}\\ < K\Big(1-\frac{1}{3}\Big)^{-1}\Big(1-\frac{1}{5}\Big)^{-1}\Big(1-\frac{1}{17}\Big)^{-1}\Big(1-\frac{1}{23}\Big)^{-1}\prod_{10 \leqq i \leqq r+5}\Big(1-\frac{1}{q_i}\Big)^{-1},\end{aligned}$$

on using Theorems 2 and 3. Hence

$$2^r < K \cdot \frac{1}{2} \cdot \frac{6}{7} \cdot \frac{10}{11} \cdot \frac{12}{13} \cdot \frac{18}{19} \cdot Q_{r+5}^{-1}$$

where Q_{r+5} is defined as in (3.2). We now use the estimate given by Rosser and Schoenfeld [3, Theorem 8, Corollary 1] for Q_{r+5}^{-1}, namely $Q_{r+5}^{-1} < e^{\gamma} \log x (1 + \log^{-2} x)$, where $x = q_{r+5}$; and obtain the stated result.

In the next theorem, q_u denotes, as already noted, the uth prime in the sequence of primes $q_1 = 2$, $q_2 = 3, \cdots$.

THEOREM 5. *Let K and m be given and let q_u be the smallest prime factor of n which is a solution of the simultaneous equations*

$$\phi(n)t(n) + 2 = Kn \tag{3.8}$$

$$t(n) = mK\,. \tag{3.9}$$

Then n has a prime factor at least as large as

$$q_u^m + O(u^m \exp - \log^b u)$$

where b is any number $< 3/5$.

Proof. We illustrate the proof for the case when n is odd. Using the lemma, we have

$$2^r \geqq K > 2^r\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$
$$> 2^r\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{17}\right)\left(1 - \frac{1}{23}\right) \cdots \left(1 - \frac{1}{p_r}\right),$$

on using part (B) of Theorem 2 and Theorem 3. Giving K successive integral values and examining the consistency of the resulting inequalities while keeping in view the restrictions of Theorem 2, we get the results of the theorem.

REMARK. Any solution n of (3.1) satisfies the relation

$$2^r < \frac{6480}{19019} K e^\gamma \log x(1 + \log^{-2} x)$$

where γ is Euler's constant, r is the number of distinct prime factors of n and $x = q_{r+5}$. To show this, we note that

$$2^r = t(n) < K\frac{n}{\phi(n)}$$
$$< K\left(1 - \frac{1}{3}\right)^{-1}\left(1 - \frac{1}{5}\right)^{-1}\left(1 - \frac{1}{17}\right)^{-1}\left(1 - \frac{1}{23}\right)^{-1} \prod_{10 \leqq i \leqq r+5}\left(1 - \frac{1}{q_i}\right)^{-1},$$

on using Theorems 2 and 3. Hence

$$2^r < K \cdot \frac{1}{2} \cdot \frac{6}{7} \cdot \frac{10}{11} \cdot \frac{12}{13} \cdot \frac{18}{19} \cdot Q_{r+5}^{-1}$$

where Q_{r+5} is defined as in (3.2). We now use the estimate given by Rosser and Schoenfeld [3, Theorem 8, Corollary 1] for Q_{r+5}^{-1}, namely $Q_{r+5}^{-1} < e^\gamma \log x(1 + \log^{-2} x)$, where $x = q_{r+5}$; and obtain the stated result.

In the next theorem, q_u denotes, as already noted, the uth prime in the sequence of primes $q_1 = 2$, $q_2 = 3, \cdots$.

THEOREM 5. *Let K and m be given and let q_u be the smallest prime factor of n which is a solution of the simultaneous equations*

$$\phi(n)t(n) + 2 = Kn \tag{3.8}$$

$$t(n) = mK\,. \tag{3.9}$$

Then n has a prime factor at least as large as

$$q_u^m + O(u^m \exp - \log^b u)$$

where b is any number $< 3/5$.

Proof. By Theorem 2, n is square free. Let it have r distinct prime divisors.

Then A. Walfisz [5, Satz 4, p. 187] has shown that if $\pi(x)$ denotes, as usual, the number of primes $\leqq x$, and

$$li\, x = \int_2^x \frac{dt}{\log t}\,,$$

then

$$\pi(x) = li(x) + O(x\{\exp - A \log^{3/5} x(\log\log x)^{-1/5}\})\,,$$

where A is a positive constant. It follows that

$$\pi(x) = li(x) + O(x \exp - \log^a x)$$

for all $a < 3/5$. By using a standard argument, we can show that

$$\sum_{q \leqq x} \frac{1}{q} = \log\log x + c + O(\exp - \log^a x)\,,$$

q varying over primes.

It follows that

$$\sum_{q \leqq x} - \log\left(1 - \frac{1}{q}\right) = \sum_{q \leqq x} \frac{1}{q} + \sum_{q} \left\{-\log\left(1 - \frac{1}{q}\right) - \frac{1}{q}\right\} + O\left(\frac{1}{x}\right)$$
$$= \log\log x + c + O(\exp - \log^a x)$$

for all $a < 3/5$, where c is an absolute constant (not necessarily the same as the c used before).

Hence for any given h for which $h = O(x^m)$, we have

$$(3.10) \qquad \sum_{x \leqq q \leqq x^m + h} - \log\left(1 - \frac{1}{q}\right)$$
$$= \log\log(x^m + h) - \log\log x + O(\exp - \log^a x)$$

for all $a < 3/5$. If we choose $h = x^m \exp(-\log^b x)$, where $b < a < 3/5$, we get

$$\sum_{x \leqq q \leqq x^m + h} - \log\left(1 - \frac{1}{q}\right) = \log m + \frac{\exp - \log^b x}{m \log x}$$
$$+ O\left\{\frac{\exp - 2\log^b x}{\log x} + O(\exp - \log^a x)\right\}\,,$$

and this is greater than $\log m$ for all sufficiently large x. Again, if we take $h = -x^m \exp(-\log^b x)$ where $b < a < 3/5$, then

$$\sum_{x \leq q \leq x^{m+h}} - \log\left(1 - \frac{1}{q}\right) = \log m - \frac{\exp(-\log^b x)}{m \log x}$$
$$+ O\left(\frac{\exp(-2\log^b x)}{\log x}\right) + O(\exp(-\log^a x)) ,$$

which is less than $\log m$ for all sufficiently large x. Hence, if $g(x)$ is the smallest number such that

$$\sum_{x \leq q \leq g(x)} - \log\left(1 - \frac{1}{q}\right) \geq \log m ,$$

then $g(x) = x^m + O(x^m \exp(-\log^a x))$ for all $a < 3/5$. Now going back to the relation

$$2^r \phi(n) + 2 = Kn .$$

This gives, with $m = 2^r/K$, the result

$$m + 2/\phi(n) = n/\phi(n) .$$

Taking q_u to be the smallest prime divisor of n, let the integer v be defined to be the smallest integer with the property

$$m < \prod_{i=u}^{v} \frac{q_i}{q_i - 1}$$

that is,

$$\sum_{q_u \leq q \leq q_v} - \log\left(1 - \frac{1}{q}\right) > \log m .$$

Then it follows that n must have a prime factor other than q_u and at least as large as q_v. The previous investigation shows that

$$q_v = q_u^m + O(q_u^m \exp(-\log^a (q_u^m))) ,$$

that is,

$$q_v = q_u^m + O(u^m \exp(-\log^b u)) \text{ for any } b < a < 3/5 .$$

Hence, we have proved the theorem.

REFERENCES

1. D. H. Lehmer, *On Euler's totient function*, Bull. Amer. Math. Soc., **38** (1932), 745-751.
2. E. Lieuwens, *Do there exist composite numbers M for which* $K\phi(M) = M - 1$ *holds?* Niew Archief von Wiskunde (3), **18** (1970), 165-169.
3. J. B. Roser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math., **6** (1962), 64-94.
4. Fr. Schuh, *Do there exist composite numbers m for which* $\phi(m) \mid m - 1$ (Dutch), Mathematica Zutphen B, **13** (1944), 102-107.

5. A. Walfisz, *Weylsche Exponential Summen in den neueren Zahlentheorie,* Veb Deutscher Verlag der Wissenschaften, Berlin, 1963.

Received May 20, 1971. Part of this research work was done at the University of Missouri during the summer of 1968. T. J. Cook, R. S. Newberry and J. M. Weber (undergraduate students there at that time) helped the author in the calculations which led to Theorem 4 of the paper.

THE UNIVERSITY OF ALBERTA