#A26 INTEGERS 10 (2010), 313-317

ON CONGRUENCE CONDITIONS FOR PRIMALITY

Sherry Gong
Departments of Mathematics and Physics, Harvard University
sgong@fas.harvard.edu

Scott Duke Kominers[1]
Department of Economics, Harvard University, and Harvard Business School
kominers@fas.harvard.edu, skominers@gmail.com

Received: 5/22/09, Revised: 2/28/10, Accepted: 3/7/10, Published: 7/16/10

Abstract

For any $k \geq 0$, all primes n satisfy the congruence $n\sigma_k(n) \equiv 2 \bmod \varphi(n)$. We show that this congruence in fact characterizes the primes, in the sense that it is satisfied by only finitely many composite n. This characterization generalizes the results of Lescot and Subbarao for the cases $k = 0$ and $k = 1$. For $0 \leq k \leq 14$, we enumerate the composite n satisfying the congruence. We also prove that any composite n which satisfies the congruence for some k satisfies it for infinitely many k.

1. Introduction

Lescot [1] and Subbarao [2] showed that, for $k \in \{0, 1\}$, the congruence

$$n\sigma_k(n) \equiv 2 \bmod \varphi(n), \tag{1}$$

in some sense characterizes the set $\mathcal{P}$ of primes. Specifically, they respectively showed the $k = 0$ and $k = 1$ cases of the following theorem.

Theorem 1. *For $k \in \{0, 1\}$ and $n \in \mathbb{N}$, the congruence* (1) *holds if and only if $n \in \mathcal{P} \cup \{1\} \cup S_k$, where $S_0 = \{4, 6, 14\}$ and $S_1 = \{4, 6, 22\}$.*

Here, σ_k and φ respectively denote the *divisor* and *totient* functions, defined by

$$\sigma_k(n) = \sum_{d|n} d^k = \prod_{i=1}^{r} \frac{p_i^{(\alpha_i+1)k} - 1}{p_i^k - 1},$$

$$\varphi(n) = |\{d \in \mathbb{N} : 1 \leq d < n \text{ and } (d, n) = 1\}| = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1),$$

for $k \geq 0$ and $\mathbb{N} \ni n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ (with the $p_i \in \mathcal{P}$ distinct).

[1] Corresponding author.

It is clear that if $n \in \mathcal{P}$, then $\sigma_k(n) = n^k + 1$ and $\varphi(n) = n - 1$. In this case, we have

$$n\sigma_k(n) \equiv n(n^k + 1) \equiv 2 \bmod (n-1),$$

as $p \equiv 1 \bmod (p-1)$. We therefore see that, for any $k \geq 0$, all $n \in \mathcal{P}$ satisfy (1).

In this note, we present the following result generalizing the reverse direction of Theorem 1.

Theorem 2. *For any $k \geq 0$, let S_k be the set of composite $n \in \mathbb{N}$ satisfying* (1). *Then,*

(i) *$S_k \subset 2\mathcal{P}$,*

(ii) *S_k is finite, and*

(iii) *the maximal element of S_k is at most $2^{k+3} + 6$.*

We prove Theorem 2 in Section 2. Then, in Section 3, we enumerate the sets S_k for $0 \leq k \leq 14$. There, we also prove that any $n \in \mathbb{N}$ which appears in S_k for some $k \geq 0$ appears in infinitely many of the sets $\{S_{k'}\}_{k'=0}^{\infty}$.

2. Proof of Theorem 2

We suppose that $n \in S_k$, i.e., that n is composite and satisfies (1). Upon writing $n = 2^\alpha p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ with the $p_i \in \mathcal{P}$ distinct and odd, we have

$$\varphi(n) = 2^{\alpha-1} \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1). \tag{2}$$

For any i ($1 \leq i \leq r$) such that $\alpha_i > 1$, we see from the expression (2) that $p_i \mid \varphi(n)$. Since clearly $p_i \mid n$, the congruence (1) then gives that $p_i \mid 2$—an impossibility. Thus, we must have $\alpha_i = 1$. An analogous argument shows that $\alpha \in \{1, 2\}$.

Now, as $p_i - 1$ is even for each i ($1 \leq i \leq r$), we see from (2) that $2^r \mid \varphi(n)$. Furthermore, the expression

$$\begin{aligned} \sigma_k(n) &= \frac{2^{(\alpha+1)k} - 1}{2^k - 1} \prod_{i=1}^{r} \frac{p_i^{(\alpha_i+1)k} - 1}{p_i^k - 1} \\ &= \frac{2^{(\alpha+1)k} - 1}{2^k - 1} \prod_{i=1}^{r} \frac{p_i^{2k} - 1}{p_i^k - 1} = \frac{2^{(\alpha+1)k} - 1}{2^k - 1} \prod_{i=1}^{r} (p_i^k + 1) \end{aligned} \tag{3}$$

yields that $2^r \mid \sigma_k(n)$ since $2 \mid p_i^k + 1$. We then obtain from the congruence (1) that $2^r \mid 2$, whence we see that $r \leq 1$.

Since n is composite, we are left with only two possibilities: $n = 2p$ (with $p \in \mathcal{P}$) or $n = 4p$ (with $p \in \mathcal{P}$). The second case is impossible, as when $n = 4p$ we have (1) and $4 \mid \varphi(n)$, together implying $4 \mid 2$; the fact that $S_k \subset 2\mathcal{P}$ follows. In the first case, if $p = 2$, then $n = 4 \leq 2^{k+3}+6$. If p is odd, then we have $n\sigma_k(n) = 2p(2^k+1)(p^k+1)$ and $\varphi(n) = p - 1$. Because $p \equiv 1 \bmod (p-1)$, we see that

$$n\sigma_k(n) \equiv 2p(2^k + 1)(p^k + 1) \equiv 4(2^k + 1) \bmod (p - 1). \tag{4}$$

Combining (1) and (4), we see that

$$(p - 1) \mid 2^{k+2} + 2. \tag{5}$$

As $n = 2p$ and (5) implies that $p \leq 2^{k+2} + 3$, we have the stated bound on the size of $n \in S_k$; the finitude of S_k follows.

3. The Sets S_k

Table 1 presents the exceptional sets S_k for $0 \leq k \leq 14$. It is clear that $4, 6 \in S_k$ for each $k \geq 0$, since $\varphi(4) = \varphi(6) = 2$, and $4\sigma_k(4)$ and $6\sigma_k(6)$ are even for all k. Beyond this observation, however, the behavior of the sets S_k appears to be quite erratic.

Nonetheless, we obtain the following partial characterization result for the S_k.

Corollary 3. *If $n \in \mathbb{N}$ is in S_k for some $k \geq 0$, then it is in infinitely many of the sets $\{S_{k'}\}_{k'=0}^{\infty}$.*

Proof. It is easily seen in the proof of Theorem 2 that $n \in S_k$ if and only if $n = 2p$ for $p \in \mathcal{P}$ satisfying

$$(p - 1) \mid (2^{k+2} + 2),$$

or equivalently,

$$\frac{p - 1}{2} \mid (2^{k+1} + 1).$$

But this means that $2^{k+1} \equiv -1 \bmod \frac{p-1}{2}$, hence $2^{2k+2} \equiv 1 \bmod \frac{p-1}{2}$. It follows that we have

$$2^{(2j+1)(k+1)-1} = 2^{(2k+2)j+k} \equiv 2^k \bmod \frac{p - 1}{2}$$

k	S_k
0	{4,6,14}
1	{4,6,22}
2	{4,6,14,38}
3	{4,6}
4	{4,6,14,46,134}
5	{4,6,22,262}
6	{4,6,14}
7	{4,6}
8	{4,6,14,38}
9	{4,6,22,166}
10	{4,6,14,2734}
11	{4,6}
12	{4,6,14}
13	{4,6,22,118,454}
14	{4,6,14,38,46,134,398,3974,14566}

Table 1: The exceptional sets S_k $(0 \leq k \leq 14)$

for any $j \in \mathbb{N}$. Then, for any $k' \in \{(2j+1)(k+1)-1\}_{j=1}^{\infty}$, we have

$$(p-1) \mid (2^{k'+2}+2),$$

hence $n \in S_{k'}$. We have therefore produced infinitely many k' such that $n \in S_{k'}$. □

References

[1] P. Lescot, *A characterisation of prime numbers*, The Mathematical Gazette **80** (1996), no. 488, 400–401.

[2] M. V. Subbarao, *On two congruences for primality*, Pacific Journal of Mathematics **52** (1974), 261–268.