A note on some congruences involving arithmetic functions

József Sándor

Hardy-Ramanujan Journal 41 (2018), 133-139 submitted 05/10/2018, accepted 18/11/2018, revised 29/11/2018

A note on some congruences involving arithmetic functions

József Sándor

To the memory of S. Srinivasan

Abstract. We consider some congruences involving arithmetical functions. For example, we study the congruences $n\psi(n) \equiv 2 \pmod{\varphi(n)}$, $n\varphi(n) \equiv 2 \pmod{\psi(n)}$, $\psi(n)d(n) - 2 \equiv 0 \pmod{n}$, where $\varphi(n)$, $\psi(n)$, $d(n)$ denote Euler's totient, Dedekind's function, and the number of divisors of n, respectively. Two duals of the Lehmer congruence $n - 1 \equiv 0 \pmod{\varphi(n)}$ are also considered.

Keywords. Euler's totient, Dedekind's arithmetical function, number of divisors, primality, congruences

2010 Mathematics Subject Classification. 11A25, 11A07, 11D45, 11N05.

1. Introduction

Apart from the classical Wilson theorem, which asserts that a positive integer $n > 1$ is a prime if and only if $(n-1)! \equiv -1 \pmod{n}$, and its variants and corollaries, there are no known simple primality conditions in the form of a congruence. The famous Lehmer congruence (see [Le32], [SáC05], [SáMC06]) is the following:

$$n - 1 \equiv 0 \pmod{\varphi(n)}. \tag{1.1}$$

This congruence is satisfied by every prime. We do not yet know if it has any composite n as a solution. (For many results, and related facts, see the monograph [SáC05]).

In 1974 M.V. Subbarao [Su74] considered the two congruences

$$n\sigma(n) \equiv 2 \pmod{\varphi(n)} \tag{1.2}$$

and

$$\varphi(n)d(n) + 2 \equiv 0 \pmod{n} \tag{1.3}$$

where φ is Euler's totient, d the number of divisors, and σ the sum of divisors functions, respectively. Each of these is satisfied whenever n is a prime, or $n = 1$. In [Su74] it is proved that the only composite solutions to (1.2) are $n = 4$, 6 and 22; while $n = 4$ is the only known such solution to (1.3). Up to $n \leq 100,000$ no other solutions are known; and if $\omega(n)$, the number of distinct prime factors of n, is fixed, then there are at most a finite number of solutions.

If in (1.2) one replaces φ by σ, we are lead to the study of the congruence

$$n\varphi(n) \equiv 2 \pmod{\sigma(n)}. \tag{1.4}$$

It is immediate that this is satisfied again when n is a prime. While $n = 8$ is a composite solution to (1.4), no general method is available to the author in order to deduce all other solutions, as in the case of equation (1.2). However, we will be able to completely solve both equations (1.2), as well as (1.4), when φ is replaced by ψ in equation (1.3) of Subbarao (and 2 with -2). In this case, we obtain another deep problem, and we will offer only a partial solution.

We thank episciences.org for providing open access hosting of the electronic journal *Hardy-Ramanujan Journal*

2. Main Results

Theorem 1. *The only composite solutions to the congruence*

$$n\psi(n) \equiv 2 \pmod{\varphi(n)} \tag{2.5}$$

are $n = 4$, 6 *and* 22.

The single composite solution to the congruence

$$n\varphi(n) \equiv 2 \pmod{\psi(n)} \tag{2.6}$$

is $n = 4$.

Proof. Let $1 < n = p_1^{a_1} \dots p_r^{a_r}$ be the prime factorization of n (p_i distinct primes, $a_i \geq 1$ integers, $i = 1, 2, ..., n$). Then

$$\varphi(n) = p_1^{a_1} \dots p_r^{a_r} \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_r}\right),$$

$$\psi(n) = p_1^{a_1} \dots p_r^{a_r} \left(1 + \frac{1}{p_1}\right) \dots \left(1 + \frac{1}{p_r}\right),$$

so we can easily deduce the following two properties of these functions (see also [Sá88]):

$$a \mid b \;\Rightarrow\; \varphi(a) \mid \varphi(b); \tag{2.7}$$

$$a \mid b \;\Rightarrow\; \psi(a) \mid \psi(b). \tag{2.8}$$

Now let p be an odd prime divisor of n in congruence (2.5), such that $p^2 \mid n$. Then by property (2.7) it follows that $\varphi(p^2) \mid \varphi(n)$, so that $p \mid \varphi(n)$. But then (2.5) implies also $p \mid 2$, which is impossible. This means that there is no $a_i > 1$ in the prime factorization $n = p_1^{a_1} \dots p_r^{a_r}$, i.e. $a_i = 1$ for all i, whenever $p_i \geq 3$. Suppose that $p_1 = 2$ and $p_j \geq 3$ for $j \geq 2$. Then n must have the form $n = 2^{a_1} p_2 \dots p_r$. Assume now that $a_1 \geq 3$. Then $2^3 \mid n$, so by (2.8), $\psi(8) = 12$ divides $\psi(n)$. Since $\varphi(8) = 4$ divides $\varphi(n)$ by (2.7), we would obtain from (2.5) that 4 divides 2, which is absurd. Therefore, we must have $a_1 \in \{0, 1, 2\}$.

(i) For $a_1 = 0$, since n is composite, we get $r \geq 3$. Then

$$\varphi(n) = (p_1 - 1) \dots (p_r - 1), \quad \psi(n) = (p_2 + 1) \dots (p_r + 1)$$

and since both these quantities are divisible by 4, this is in contradiction with congruence (2.5).

(ii) For $a_1 = 1$,

$$\varphi(n) = (p_2 - 1) \dots (p_r - 1), \quad \psi(n) = 3(p_2 + 1) \dots (p_r + 1)$$

and again we cannot have $r \geq 3$, so $r = 2$, when $n = 2p_2$. For $\varphi(n) = p_2 - 1$, $\psi(n) = 3(p_2 + 1)$, we get the congruence

$$6p_2(p_2 + 1) \equiv 2 \pmod{p_2 - 1}. \tag{2.9}$$

As $6p_2(p_2 + 1) = 6(p_2 - 1 + 1)(p_2 - 1 + 2)$, this is possible only when

$$10 \equiv 0 \pmod{p_2 - 1}. \tag{2.10}$$

The solutions of (2.10) are given by $p_2 - 1 = 2$, 10 (as $p_2 - 1$ is even) so $p_2 = 3$, 11. These provide the solutions $n = 6$, 22.

(iii) For $a_2 = 2$ we get $n = 4p_2$ so $4 \mid \psi(n), \varphi(n)$, which is in contradiction with congruence (2.5). We have not considered the case where no odd prime factors exist; then clearly $n = 2^{a_1}$, with

$a_1 \in \{0,1,2\}$ and only $a_1 = 2$ is acceptable. So $n = 4$ is a solution of this type. This finishes the proof of the first part of Theorem 1.

For equation (2.6) we can repeat the same argument as above. The solutions can only be 4, $2p_2$ or $4p_2$. By $\varphi(2p_2) = p_2 - 1$, $\psi(2p_2) = 3(p_2+1)$, (2.6) would imply $2[p_2(p_2-1)-1]$ divisible by $3(p_2+1)$, and since $p_2(p_2-1)-1 = (p_2+1-1)(p_2+1-2)-1 \equiv 1 \pmod{(p_2+1)}$, this is impossible. Similarly, for $\varphi(4p_2) = 2(p_2-1)$, $\psi(4p_2) = 6(p_2+1)$ both are divisible by 4, a contradiction.

The remaining number $n = 4$, however is a solution; and the proof of Theorem 1 is completed.

Theorem 2. *All primes satisfy the congruence*

$$\psi(n)d(n) \equiv 2 \pmod{n}. \tag{2.11}$$

Suppose that $n > 4$ is a composite solution. Then:

1) n must be squarefree.

2) There are a finite number of solutions n with $\omega(n)$ fixed.

3) If $\psi(n)d(n) - 2 = K \cdot n$, and n is odd, then K is even and $2 \,||\, K$. If n is even, then K is odd and $3 \nmid K$, $3 \nmid n$. If $3 \mid n$, then $4 \nmid K$, $4 \nmid n$.

More generally, if $p \mid n$, then $p+1 \nmid K, n$.

Proof. As $\psi(p)d(p) = 2(p+1) \equiv 2 \pmod{p}$, the primes $n = p$ are solutions to congruence (2.11). If m is the odd part of n, and $p^2 | m$, then by (2.8) $p \mid \psi(m)$ so (2.11) becomes impossible, as $p \nmid 2$. Let $n = 2^k m$, where m is odd. Then $\psi(n) = 2^{k-1} \cdot 3\psi(m)$. Supposing $m = 1$, one gets the solutions $n = 2$, 4 to (2.11). Since $n > 4$, we must have $m \geq 3$. But it then easily follows from the definition of function ψ that $\psi(m)$ is even. Thus $\psi(n)$ is divisible by 2^k, contradicting (2.11), when $n \geq 2$. This shows that n must be squarefree.

Let now $\omega(n) = r$ be fixed, and write

$$\psi(n)d(n) - 2 = K \cdot n,$$

when $n = q_1 q_2 \dots q_r$, so $d(n) = 2^r$.

Then

$$K = \frac{(q_1+1)\dots(q_r+1)\cdot 2^r - 2}{q_1 \dots q_r} > 2^r,$$

$$2^r[(q_1+1)\dots(q_r+1) - q_1 \dots q_r] > 2,$$

which follows by $r > 1$ and $(q_1+1)\dots(q_r+1) - q_1 \dots q_r > 1$.

On the other hand, as

$$K < 2^r \cdot \frac{\psi(n)}{n} = 2^r \left(1 + \frac{1}{q_1}\right) \dots \left(1 + \frac{1}{q_r}\right)$$

(where q_i $(i = 1, 2, ..., n)$ are the distinct prime divisors of n) we can write

$$K < 2^r \left(1 + \frac{1}{p_1}\right) \dots \left(1 + \frac{1}{p_r}\right), \tag{2.12}$$

where p_i $(i = 1, 2, ..., n)$ denotes the ith prime number. (Clearly $q_1 \geq p_1, \dots, q_r \geq p_r$). Since

$$\prod_{p \leq x} \left(1 + \frac{1}{p}\right) < \frac{1}{\prod_{p \leq x} \left(1 - \frac{1}{p}\right)},$$

and by Mertens' theorem (see [SáMC06])

$$\prod_{p\le x}\left(1-\frac{1}{p}\right)>\frac{c}{\log x}$$

($c>0$, p runs through the primes), we get from (2.12) that

$$K<\frac{1}{C}\cdot 2^r\log p_r$$

so, as r is fixed, K can only take a finite number of values.

Now, by the arithmetic mean - geometric mean inequality one can derive

$$\left(1+\frac{1}{q_1}\right)\dots\left(1+\frac{1}{q_r}\right)<\left(1+\frac{1}{r}\left(\frac{1}{q_1}+\dots+\frac{1}{q_r}\right)\right)^r,$$

so by (2.12) one has

$$r\left(\frac{K^{1/r}}{2}-1\right)<\frac{1}{q_1}+\dots+\frac{1}{q_r}. \tag{2.13}$$

(Here $\frac{K^{1/r}}{2}-1>0$, as $K>2^r$, see above). As $\frac{1}{q_1}+\dots+\frac{1}{q_r}<\frac{r}{q_1}$, we get that by (2.13),

$$q_1<\frac{1}{K^{1/2}/2-1}=f_1(K,r)>0.$$

Now, by (2.13),

$$r\left(\frac{K^{1/2}}{2}-1\right)-\frac{1}{q_1}<\frac{1}{q_2}+\dots+\frac{1}{q_r}<\frac{r-1}{q_2},$$

so

$$q_2<\frac{r-1}{r/f_1(K,r)+\frac{1}{q_1}}=f_2(K,r)>0;$$

and continuing in this way, we can proceed inductively, and obtain

$$q_r<1/\left(\frac{1}{q_1}+\dots+\frac{1}{q_{r-1}}-r\left(\frac{K^{1/r}}{2}-1\right)\right);$$

so if $q_1,\dots,q_{r-1}$ can take at most a finite number of values, this is also true for q_r.

Part 2) of Theorem 2 is proved as $n=q_1\dots q_r$.

Now, to prove the assertions of part 3) remark that $\psi(n)\cdot 2^r-2=K\cdot n$, so if n is odd, then clearly K must be even (but $2\,||\,K$). If n is even, then K is odd, as $2\,||$ left side. Since $2\mid n$, we have $3\mid\psi(n)$, so $3\nmid K$, $3\nmid n$. Generally, $p\mid n$ implies $p+1\mid\psi(n)$, and since $p+1\nmid 2$, we clearly have that $p+1\nmid K,n$.

3. Other congruences

Theorem 3. *The only solutions $n>1$ to the congruence*

$$\varphi(n)\sigma(n)+1\equiv 0\pmod{n^2} \tag{3.14}$$

are the prime numbers.

Proof. Let $p < n = p_1^{a_1} \dots p_r^{a_r}$ be the prime factorization of n. Then it is clear that

$$\varphi(n)\sigma(n) - n^2 = p_1^{\alpha_1 - 1} \dots p_r^{\alpha_r - 1}[(p_1^{\alpha_1+1} - 1) \dots (p_r^{\alpha_r+1} - 1) - p_1^{\alpha_1+1} \dots p_r^{\alpha_r+1}],$$

by an easy computation. Now remark that by letting $p_i^{\alpha_i+1} - 1 = x_i$, we have

$$(x_1 - 1) \dots (x_r - 1) - x_1 \dots x_r \leq -1$$

(i.e., since $x_i > 1$, by letting $x_i - 1 = y_i > 0$, $(y_1 + 1) \dots (y_r + 1) \geq y_1 \dots y_r + 1$; trivial), with equality only for $r = 1$; and since $p_1^{\alpha_1 - 1} \dots p_r^{\alpha_r - 1} \geq 1$, with equality only when $\alpha_1 = \dots = \alpha_r = 1$, we get that

$$\varphi(n)\sigma(n) \leq n^2 - 1 \tag{3.15}$$

with equality only for $n =$ prime. Since $\varphi(n)\sigma(n) + 1 \leq n^2$, this means that (3.14) holds only when there is equality in (3.15); so only for the prime numbers.

Theorem 4. *If $n > 1$ is a composite solution to the congruence*

$$\varphi(n)\sigma(n) + 1 \equiv 0 \pmod{n}, \tag{3.16}$$

then n is odd and squarefree. All prime numbers are solutions.

Proof. Observe that $n = p$ prime, is a solution, since

$$(p - 1)(p + 1) + 1 = p^2 \equiv 0 \pmod{p}.$$

Let n be a composite solution. Then, n cannot be even, as for $n \geq 4$ it is well-known that $\varphi(n)$ is even, so the left side of (3.16) is odd. If n is odd, let p be a prime divisor of n such that $p^2 \mid n$. By (2.7) we get that $p \mid \varphi(n)$, so $p \mid 1$ in (3.16), a contradiction.

As we have seen in the Introduction, the famous Lehmer problem states that $n - 1 \equiv 0 \pmod{\varphi(n)}$ doesn't have composite solutions. The congruence

$$\psi(n) - 1 \equiv 0 \pmod{n} \tag{3.17}$$

could be named as a **"dual" of the Lehmer problem**. (Indeed, $\psi(n) = n \prod_{p \mid n} \left(1 + \frac{1}{p}\right)$ is a kind of dual of $\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$, and $n \mid (\psi(n) - 1)$ may be considered as a reciprocal dual of $\varphi(n) \mid (n - 1)$).

Theorem 5. *Any prime number satisfies the congruence (3.17). If $n > 1$ is a composite solution, then n is odd and squarefree. There are at most a finite number of solutions for a fixed value of $\omega(n)$. If n is a solution, then $\omega(n) \geq 18$.*

Proof. Since for $n = p$ (prime), $\psi(n) = p + 1$, clearly the primes satisfy (3.17). Now, if $n \geq 4$ is a composite solution, then as $\psi(n)$ is even, $\psi(n) - 1$ being odd, cannot have even divisors, so n is odd. If $p \mid n$ is an odd prime such that $p^2 \mid n$, then $p \mid \psi(n)$, contradicting (3.17). If $\omega(n) = r$ fixed, then $\psi(n) - 1 = K \cdot n$, and the number of solutions will be finite, which can be shown almost in the same manner as in the proof of Theorem 2 (we omit the details). Now, write (3.17) as

$$\psi(n) = K \cdot n + 1. \tag{3.18}$$

For n odd composite, $\psi(n)$ is even, and n is odd. Thus K must be odd, too. This means that $K \geq 3$ ($K = 1$ is impossible, as $\psi(n) = n + 1$ would imply $n =$ prime, as $\psi(n) \geq n + 1$, with equality

only for primes). We will show that when $\omega(n) \leq 17$, we have $\psi(n) < 3n$, contradicting $K \geq 3$ in (3.18).

Set $n = q_1 \dots q_r$. Then

$$\frac{\psi(n)}{n} = \left(1+\frac{1}{q_1}\right)\dots\left(1+\frac{1}{q_r}\right) \leq \left(1+\frac{1}{p_1}\right)\dots\left(1+\frac{1}{p_r}\right),$$

where p_i is the ith prime number.

Let $r \leq 17$. Then

$$\frac{\psi(n)}{n} \leq \left(1+\frac{1}{p_1}\right)\dots\left(1+\frac{1}{p_r}\right) \leq \left(1+\frac{1}{p_1}\right)\dots\left(1+\frac{1}{p_{17}}\right)$$
$$= \frac{4}{3}\cdot\frac{6}{5}\cdot\frac{8}{7}\cdot\frac{12}{11}\cdot\frac{14}{13}\cdot\frac{18}{17}\cdot\frac{20}{19}\cdot\frac{24}{23}\cdot\frac{30}{29}\cdot\frac{32}{31}\cdot\frac{38}{37}\cdot\frac{42}{41}\cdot\frac{44}{43}\cdot\frac{48}{47}\cdot\frac{54}{53}\cdot\frac{60}{59}\cdot\frac{62}{61} \approx 2.9\dots,$$

with the aid of a computer. Thus $\frac{\psi(n)}{n} < 3$, in contradiction to $\frac{\psi(n)}{n} \geq 3 + \frac{1}{n}$.

Remark. A similar dual could be obtained when ψ is replaced by σ. The obtained congruence

$$\sigma(n) - 1 \equiv 0 \pmod{n} \tag{3.19}$$

is related also to the congruence

$$\sigma(n) \equiv 0 \pmod{n}, \tag{3.20}$$

representing to so-called "multiply perfect numbers" (see [SáC05]). It is not known if (3.20) has infinitely many solutions.

Theorem 6. *Any prime number satisfies congruence (3.19). If n is a composite solution, then n must be abundant. There are a finite number of solutions n with $\omega(n)$ fixed.*

Proof. For $n = p$ one has $\sigma(n) - 1 = p \equiv 0 \pmod{p}$. Put

$$\sigma(n) - 1 = K \cdot n. \tag{3.21}$$

Thus, if n is composite, then $K = 1$ is impossible, as $\sigma(n) = n + 1$ would imply $n =$ prime. Therefore $K \geq 2$, so $\sigma(n) \geq 2n + 1 > 2n$, i.e. n is abundant number.

Remark. If $K = 2$ in (3.21), then n is called a **quasiperfect** number. It is not known if such numbers exist (see [SáC05], [SáMC06] with other results).

Let now $\omega(n) = r$ be fixed. In [Sá89] it is proved that

$$\sigma(n) \leq n(\omega(n) + 1). \tag{3.22}$$

By (3.22) we get $\frac{\sigma(n)}{n} \leq r + 1$, so $\frac{\sigma(n)}{n}$ can take at most a finite number of values. Thus,

$$K = \frac{\sigma(n)}{n} - \frac{1}{n} < \frac{\sigma(n)}{n},$$

i.e. K has a finite number of values.

For a fixed value of K in (3.21) we get a fixed equation, which is a "quasi-perfect" type. H.J. Kanold (see [Ka88]) has shown that there are at most a finite number of quasi-perfect numbers with $\omega(n) = r$. His method can be slightly changed in order to obtain the similar result with fixed K (in place of $K = 2$). We omit the details.

Final remarks. A computer search revealed that, up to 100,000, the only solutions, besides the primes, to relations (3.16), (3.17) and (3.19) are $n = 1$. For (1.4) the only solutions are $n = 1, 8, 9$; while for relation (2.11) we know the following solutions: $n = 1, 4, 10, 21, 1462, 4342, 29491$. The author cannot decide if the number of solutions is finite or infinite.

Acknowledgment. The author is grateful to the referee for suggestions which have improved the presentation of the paper.

References

[Ka88] H. -J. Kanold, Über quasi-vollkommene Zahlen, *Ab. Braunschweig, Wiss. Ges.* **40** (1988), 17-20.

[Le32] D. H. Lehmer, On Euler's totient function, *Bull. Amer. Math. Soc.* **38** (1932), 745-751.

[Sá88] J. Sándor, On Dedekind's arithmetical function, *Seminarul de t. structurilor, no.51*, 1988, Univ. Timişoara.

[Sá89] J. Sándor, On some diophantine equations for particular arithmetic functions (Romanian), *Seminarul de t. structurilor, no.53*, 1989, Univ. Timişoara.

[Su74] M. V. Subbarao, On two congruences for primality, *Pacific J. Math.* **52** (1974), 261-268.

[SáC05] J. Sándor and B. Crstici, *Handbook of number theory II*, Springer Verlag, 2005.

[SáMC06] J. Sándor, D. S. Mitrinović and B. Crstici, *Handbook of number theory I*, Springer Verlag, 2006.

József Sándor
Department of Mathematics
Babeş-Bolyai University
Romania. *e-mail*: jsandor@math.ubbcluj.ro