# ON A CONJECTURE OF DEACONESCU

**Elchin Hasanalizade**[1]
*Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, Canada*
e.hasanalizade@uleth.ca

*Received: 5/7/22, Accepted: 10/14/22, Published: 11/4/22*

**Abstract**

In 2000 Deaconescu raised a question about whether there exists a composite $n$ for which $S_2(n)|(\phi(n)-1)$, where $\phi(n)$ is Euler's function and $S_2(n)$ is Schemmel's totient function. In this paper we prove that any such $n$ is odd, squarefree and has at least seven distinct prime factors. We also prove that any such $n$ with exactly $K$ distinct prime divisors is necessarily less than $2^{2^{K+1}}$.

## 1. Introduction

Let $\phi$ denote Euler's totient function. In 1932 Lehmer [7] conjectured that if $\phi(n)|(n-1)$, then $n$ has to be a prime number. A composite positive integer satisfying that divisibility is called a *Lehmer number* or number with the *Lehmer property*. Although this problem has not been settled so far, several partial results are known. Lehmer himself proved that if $n$ has Lehmer property then $n$ is odd, squarefree and has at least seven distinct prime factors. Cohen and Hagis [3], using computational methods, established that $\omega(n) \geq 14$, where $\omega(n)$ denotes the number of distinct prime divisors of $n$. Burcsi et al. [1] showed that if, additionally, $3|n$, then $\omega(n) \geq 40 \cdot 10^6$ and $n > 10^{36 \cdot 10^7}$. On the other hand, Pomerance [9] proved that every Lehmer number $n$ is less than $K^{2^K}$, where $K = \omega(n)$. Recently, Burek and Żmija [2] improved this upper bound to $2^{2^K} - 2^{2^{K-1}}$.

In 2000 Deaconescu [4] conjectured that for $n \geq 2$

$$S_2(n)|(\phi(n)-1)$$

if and only if $n$ is prime, where $S_2(n)$ is *Schemmel's totient function*, a multiplicative

[1] This research was supported by NSERC Discovery grants RGPIN-2020-06731 of Habiba Kadiri and RGPIN-2020-06032 of Nathan Ng.

function defined by

$$S_2(p^\alpha) = \begin{cases} 0, & \text{if } \ p = 2; \\ p^{\alpha-1}(p-2) & \text{if } p > 2 \end{cases}$$

for all primes $p$ and positive integers $\alpha$.

This problem seems to be as challenging as Lehmer's problem. Clearly, the conjecture states that for every $M \geq 1$, the set $D_M$ of integers satisfying

$$MS_2(n) = \phi(n) - 1 \tag{1}$$

contains only prime numbers. We say that a composite integer $n$ is a *Deaconescu number* (or has the *Deaconescu property*) if it satisfies (1).

In this short note we prove the following results.

**Theorem 1.** *If $n$ is a Deaconescu number, then $n$ is odd, squarefree and $\omega(n) \geq 7$.*

Inspired by the work of Burek and Żmija we will also get an upper bound for Deaconescu numbers.

**Theorem 2.** *If $n$ has the Deaconescu property, then*

$$n < 2^{2^K + K} - 2^{2^{K-1} + K},$$

*where $K = \omega(n)$.*

Hernandez and Luca [6] proved that there are at most finitely many Lehmer numbers $n$ such that $P(\phi(n)) \equiv 0 \pmod{n}$, where $P(X) \in \mathbb{Z}[X]$ is any monic non-constant polynomial. We will prove the analogous result for Deaconescu numbers.

**Theorem 3.** *Let $P(X) \in \mathbb{Z}[X]$ be a monic non-constant polynomial. Then there are at most finitely many composite integers $n$ such that $S_2(n) | (\phi(n) - 1)$ and $P(S_2(n)) \equiv 0 \ (mod \ \phi(n))$.*

## 2. Preliminaries

In this section we shall collect some preliminary results. First, we give a group-theoretic interpretation of Schemmel's totient function.

**Definition 1.** Ler $R$ be a commutative ring with identity and $R^*$ be the multiplicative group of its units. A unit $u \in R$ is called *exceptional* if $1 - u \in R^*$.

Let $R^{**}$ denote the set of all exceptional units in $R$. In particular if $R = \mathbb{Z}_n$, the ring of residue classes mod $n$, then by definition we have

$$\mathbb{Z}_n^{**} = \{a \in \mathbb{Z}_n : \ \gcd(a, n) = 1 \text{ and } \gcd(a - 1, n) = 1\}.$$

In 2010, Harrington and Jones [5] proved that

$$|\mathbb{Z}_n^{**}| = S_2(n).$$

Note that $\phi(n)$ is always even if $n > 2$. Thus $M$ in (1) must be odd.

**Lemma 1.** *We have $n \in D_1$ if and only if $n = p$ for some prime $p$.*

*Proof.* If $n = p$, it is in $D_1$. If $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ $(r > 1)$ with $p_1 < p_2 < \dots p_r$ then $S_2(n) < \phi(n) - 1$ since $1 \in \mathbb{Z}_n^*$ and $p_1 + 1 \in \mathbb{Z}_n^*$ but $1 \notin \mathbb{Z}_n^{**}$ and $p_1 + 1 \notin \mathbb{Z}_n^{**}$. □

From now on we assume that $M > 1$ and that $n$ denotes an integer greater than 1 in $D_M$ for some $M > 1$. Then we have

$$\frac{\phi(n)}{S_2(n)} > M \geq 3. \tag{2}$$

The next lemma due to Nielsen [8] plays an important role in the proof of the upper bound for numbers with the Deaconescu property.

**Lemma 2.** *Let $r, a, b \in \mathbb{N}$ and let $x_1, \dots, x_r$ be integers such that $1 < x_1 < x_2 < \dots < x_r$ and*

$$\prod_{j=1}^{r} \left(1 - \frac{1}{x_j}\right) \leq \frac{a}{b} < \prod_{j=1}^{r-1} \left(1 - \frac{1}{x_j}\right). \tag{3}$$

*Then*

$$a \prod_{j=1}^{r} x_j \leq (a+1)^{2^r} - (a+1)^{2^{r-1}}. \tag{4}$$

## 3. Proofs

*Proof of Theorem 1.* By definition of $S_2(n)$ it is clear that $n$ must be odd. If $n$ is not squarefree then $n$ has a prime factor $p_i$ for which $p_i | \phi(n)$ and $p_i | S_2(n)$. In this case, if $n$ is a Deaconescu number, then $p_i | 1$ which is impossible. Next, we show that $\omega(n) \neq 2$. When $n = p_1 p_2$, Equation (1) becomes

$$M(p_1 - 2)(p_2 - 2) = (p_1 - 1)(p_2 - 1) - 1 \text{ or } M - 1 = \frac{1}{p_1 - 2} + \frac{1}{p_2 - 2}.$$

Hence $0 < M - 1 \leq 1 + \frac{1}{3} = \frac{4}{3}$ and $M = 2$, which is impossible since $M$ is odd. If $2 < \omega(n) \leq 6$, then $M = 3$ and $3 | n$. Indeed, if $n = p_1 p_2 \dots p_r$ with $p_1 < p_2 < \dots < p_r$, then (2) gives $M < \frac{\phi(n)}{S_2(n)} \leq \prod_{i=1}^{r} \frac{q_i - 1}{q_i - 2} = Q_r$, where $\{q_i\} = \{3, 5, 7, \dots\}$

denotes the sequence of all odd primes. Since $Q_r < 5$ for $2 < r \le 6$, we get $M = 3$. If $2 < r \le 6$ and $3 \nmid n$, then

$$\frac{\phi(n)}{S_2(n)} = \prod_{i=1}^{r} \frac{p_i - 1}{p_i - 2} \le \prod_{i=1}^{6} \frac{q_{i+1} - 1}{q_{i+1} - 2} < 3$$

contradicting (2). Hence $3|n$. But if $n = 3p_2 \dots p_r$ and $M = 3$, Equation (1) becomes

$$3(p_2 - 2) \cdots (p_r - 2) = 2(p_2 - 1) \cdots (p_r - 1) - 1.$$

Taking this equation modulo 3 we see that it has no solutions in primes. Hence $\omega(n) \ge 7$. □

*Proof of Theorem 1.2.* Let us write $n = p_1 \cdots p_K$ where $p_1 < p_2 < \ldots < p_K$. Then

$$\prod_{j=1}^{K} \left(1 - \frac{1}{p_j - 1}\right) = \frac{S_2(n)}{\phi(n)} < \frac{S_2(n)}{\phi(n) - 1}.$$

Moreover,

$$\begin{aligned}
\frac{\frac{S_2(n)}{\phi(n)-1}}{\prod\limits_{j=1}^{K-1}\left(1 - \frac{1}{p_j-1}\right)} &= \frac{n \prod\limits_{j=1}^{K}\left(1 - \frac{2}{p_j}\right)}{(\phi(n) - 1) \prod\limits_{j=1}^{K-1}\left(1 - \frac{1}{p_j-1}\right)} \\
&= \frac{n \prod\limits_{j=1}^{K-1}\left(1 - \frac{2}{p_j}\right)\left(1 - \frac{2}{p_K}\right)}{(\phi(n) - 1) \prod\limits_{j=1}^{K-1}\left(1 - \frac{1}{p_j-1}\right)} = \frac{n \prod\limits_{j=1}^{K-1}\left(1 - \frac{1}{p_j}\right)\left(1 - \frac{2}{p_K}\right)}{\phi(n) - 1} \\
&= \frac{\phi(n)}{\phi(n) - 1} \cdot \frac{\left(1 - \frac{2}{p_K}\right)}{\left(1 - \frac{1}{p_K}\right)} < 1
\end{aligned}$$

since $\phi(n) > p_K - 1$. Thus

$$\prod_{j=1}^{K} \left(1 - \frac{1}{p_j - 1}\right) < \frac{S_2(n)}{\phi(n) - 1} < \prod_{j=1}^{K-1} \left(1 - \frac{1}{p_j - 1}\right).$$

Hence, the inequality (3) is satisfied for $x_j = p_j - 1$, $r = K$, $a = 1$, $b = \frac{\phi(n)-1}{S_2(n)}$. From (4) we get

$$(p_1 - 1) \ldots (p_K - 1) \le 2^{2^K} - 2^{2^{K-1}}.$$

Since $p-1 > \frac{p}{2}$ for all primes $p \geq 3$, we have

$$n = p_1 \cdots p_K < 2^{2^K+K} - 2^{2^{K-1}+K}.$$

□

*Proof of Theorem 1.3.* We follow closely an argument in [6]. Let

$$P(X) = X^d + a_1 X^{d-1} + \ldots + a_d \in \mathbb{Z}[X]$$

with $d \geq 1$. Suppose $n$ is a Deaconescu number. It is known that there exists a positive constant $c$ such that $S_2(n) \geq \frac{cn}{(\log\log 3n)^2}$ for all odd $n$ (see [10]). Then

$$M \ll (\log\log n)^2. \tag{5}$$

Since $P(S_2(n)) \equiv 0 \pmod{\phi(n)}$ we have that $M^d P(S_2(n)) \equiv 0 \pmod{\phi(n)}$. Thus by (1), we get

$$(-1)^d + a_1 M(-1)^{d-1} + \ldots + a_d M^d \equiv 0 (\bmod\ \phi(n)).$$

Let $S$ denote the left hand side of the above congruence. Now we consider two case:
*Case I.* $S \neq 0$. Note that $\phi(n) \geq \sqrt{n}$ for all odd $n$. Then from the above congruence and (5), we have that

$$\sqrt{n} \leq \phi(n) \leq |S| < \left(1 + \sum_{j=1}^{d} |a_j|\right) M^d \ll (\log\log n)^{2d}$$

which implies $n \ll 1$, as we want.
*Case II.* $S = 0$. Then $(-1)^d + a_1 M(-1)^{d-1} + \ldots + a_d M^d = 0$ or

$$\left(-\frac{1}{M}\right)^d + a_1\left(-\frac{1}{M}\right)^{d-1} + \ldots + a_d = 0$$

or $P\left(-\frac{1}{M}\right) = 0$. Thus we get that $-\frac{1}{M}$ is both an algebraic integer and a rational number which is impossible since $M \geq 3$. □

## References


[1] P. Burcsi, S. Czirbusz and G. Farkas, Computational investigation of Lehmer's totient problem, *Ann. Univ. Sci. Budapest. Sect. Comput.* **35** (2011), 43–49.

[2] D. Burek and B. Żmija, A new upper bound for numbers with the Lehmer property and its application to repunit numbers, *Int. J. Number Theory* **15** (2019), no. 7, 1463–1468.

[3] G. L. Cohen and P. Hagis, On the number of prime factors of $n$ if $\phi(n)|(n-1)$, *Nieuw. Arch. Wisk. (3)* **28** (1980), no. 2, 177–185.

[4] M. Deaconescu, Adding units mod $n$, *Elem. Math.* **55** (2000), no. 3, 123–127.

[5] J. Harrington and L. Jones, On the iteration of a function related to Euler's $\phi$ function, *Integers* **10** (2010), #A42.

[6] S. H. Hernandez and F. Luca, A note on Deaconescu's result concerning Lehmer's problem, *Integers* **8** (2008), #A12.

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

[8] P. Nielsen, Odd perfect numbers, Diophantine equations, and upper bounds, *Math. Comp.* **84** (2015), 2549–2567.

[9] C. Pomerance, On composite $n$ for which $\phi(n)|n-1$, II, *Pacific J. Math.* **69** (1977), no. 2, 177–186.

[10] L.-W. Yip, *On Carmichael Type Problems for the Schemmel Totients and Some Related Questions*, Thesis (Ph.D), University of Alberta (Canada), 1989.