



HAL
open science

A NEW CHARACTERIZATION FOR THE LUCAS-CARMICHAEL INTEGERS AND SUMS OF BASE- p DIGITS

Sridhar Tamilvanan, Subramani Muthukrishnan

► **To cite this version:**

Sridhar Tamilvanan, Subramani Muthukrishnan. A NEW CHARACTERIZATION FOR THE LUCAS-CARMICHAEL INTEGERS AND SUMS OF BASE- p DIGITS. 2024. hal-04393524

HAL Id: hal-04393524

<https://hal.science/hal-04393524v1>

Preprint submitted on 14 Jan 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

A NEW CHARACTERIZATION FOR THE LUCAS-CARMICHAEL INTEGERS AND SUMS OF BASE- p DIGITS

SRIDHAR TAMILVANAN ⁽¹⁾ AND SUBRAMANI MUTHUKRISHNAN ⁽²⁾

ABSTRACT. In this paper, we prove a necessary and sufficient condition for the Lucas-Carmichael integers in terms of the sum of base- p digits. We also study some interesting properties of such integers. Finally, we prove that there are infinitely many Lucas-Carmichael integers assuming the prime k -tuples conjecture.

1. INTRODUCTION

The classical Fermat's little theorem states that if p is a prime number, then any positive integer a satisfies $a^p \equiv a \pmod{p}$. In particular, if a is not divisible by p , we have $a^{p-1} \equiv 1 \pmod{p}$. However, the converse of Fermat's little theorem is not true. For an example, 561 is the least composite integer that satisfies $a^{560} \equiv 1 \pmod{561}$ for every positive integer a with $\gcd(a, 561) = 1$. Such integers are called Carmichael integers. In general, we have the following definition:

Definition 1.1. A composite positive integer m is called a Carmichael number if the congruence $a^{m-1} \equiv 1 \pmod{m}$ holds for all integers a co-prime to m .

In 1899, A. Korselt [4] observed an important criterion for Carmichael numbers.

Theorem 1.1. (Korselt's criterion). A composite number m is a Carmichael number if and only if m is square-free and every prime divisor p of m satisfies $p - 1 \mid m - 1$.

Later, R. D. Carmichael [2, 3] proved a few interesting properties for Carmichael numbers.

Theorem 1.2. (R. D. Carmichael). Every Carmichael number m is odd, square-free and has at least three prime factors. If p and q are prime divisors of m , then

$$(i) \ p - 1 \mid m - 1, \quad (ii) \ p - 1 \mid \frac{m}{p} - 1 \quad \text{and} \quad (iii) \ p \nmid q - 1.$$

2020 *Mathematics Subject Classification.* 11A51, 11N25.

Key words and phrases. Fermat's little theorem, Carmichael number, Lucas-Carmichael integers, sum of base- p digits, Prime k -tuples Conjecture.

In 1994, W. R. Alford, Andrew Granville, and Carl Pomerance [6] solved the long-standing conjecture that the set of all Carmichael numbers is infinite. More precisely, they showed that if $C(x)$ denotes the number of Carmichael numbers less than x , then $C(x) > x^{2/7}$ for sufficiently large x .

Recently, B. C. Kellner and J. Sondow [7] derived a new characterization for Carmichael numbers as follows: For a positive integer m , denote $S_p(m)$ as the sum of the base- p digits of m . Then, m is a Carmichael number if and only if it is square-free and each of its prime factors p satisfies $S_p(m) \geq p$ and $S_p(m) \equiv 1 \pmod{p-1}$. In particular, a primary Carmichael number m is a Carmichael number that satisfies $S_p(m) = p$ for every prime factor p of m . B. C. Kellner and J. Sondow [7] counted the Carmichael numbers and primary Carmichael numbers up to 10^{10} . In 2022, Wagstaff [1] proved that the prime k -tuples conjecture implies that there are infinitely many primary Carmichael numbers.

In this paper, we study a variation of Carmichael numbers motivated by Gordon's primality testing algorithm [9] as explained below. An elliptic curve E over \mathbb{Q} is a smooth projective curve that satisfies the Weierstrass equation

$$E : Y^2 = X^3 + aX + b,$$

where $a, b \in \mathbb{Q}$ and discriminant $\Delta = 4a^3 + 27b^2 \neq 0$. For an elliptic curve E with complex multiplication by $\mathbb{Q}(\sqrt{-d})$, let $P \in E(\mathbb{Q})$ be a rational point of infinite order and m be a positive integer such that $\gcd(m, 6\Delta) = 1$ with $\left(\frac{-d}{m}\right) = -1$, where $\left(\frac{-d}{m}\right)$ is the Jacobi symbol. If m is a prime, then

$$[m+1]P \equiv \mathcal{O} \pmod{m}.$$

If m satisfies the above congruence, then m is a probable prime by Gordon's primality test. Also, m is a composite number when m does not satisfy the above congruence relation.

Definition 1.2. Let m be a composite number and E be a CM -elliptic curve. If m satisfies the Gordon primality test, then m is called an E -elliptic Carmichael number. A composite integer m is said to be an elliptic Carmichael number if m is an E -elliptic Carmichael number for every CM -elliptic curve E .

Ekstrom et al. [10] computed the following smallest elliptic Carmichael number:

$$617730918224831720922772642603971311 = p(2p+1)(3p+2),$$

where $p = 468686771783$. Also, they proved the following Elliptic Carmichael condition.

Theorem 1.3. (Elliptic Carmichael Condition). Let m be a square-free, composite positive integer with an odd number of prime factors. Moreover, let $\alpha = 8 \cdot 3 \cdot 7 \cdot 11 \cdot 19 \cdot 43 \cdot 67 \cdot 163$. Then m is an elliptic Carmichael number if for each prime $p \mid m$, we have $\alpha \mid p + 1$ and $p + 1 \mid m + 1$.

Observing the above elliptic Carmichael condition, the following Korselt-like criterion has been noted: $p + 1 \mid m + 1$ whenever $p \mid m$, and thus the Lucas-Carmichael integers have been defined.

Definition 1.3. A Lucas-Carmichael integer is a square-free positive composite integer m such that $p + 1 \mid m + 1$ whenever $p \mid m$.

In 2018, Thomas Wright [8] proved that there are infinitely many Lucas-Carmichael integers. In fact, he showed that if $\mathcal{N}(X)$ denotes the number of elliptic Carmichael numbers up to X , then there exists a constant $K > 0$ such that

$$\mathcal{N}(X) \gg (X)^{\frac{K}{(\log \log \log X)^2}}.$$

In this paper, we derive a new characterization for the Lucas-Carmichael integers and prove that there are infinitely many Lucas-Carmichael integers assuming the prime k -tuples conjecture.

2. PRELIMINARIES

We start with interesting and elementary results.

Lemma 2.1. Let m, n be two positive integers with $n > m$. Then $S_{m+1}(n + 1) \equiv n + 1 \pmod{m}$.

Proof. We write the integer $n + 1$ with respect to the base $m + 1$ as follows:

$$n + 1 = n_0 + n_1(m + 1) + n_2(m + 1)^2 + n_3(m + 1)^3 + \cdots, \quad (1)$$

where $0 \leq n_i < m + 1$ for all i .

Since $(m + 1)^k \equiv 1 \pmod{m}$ for all positive integer k and from the equation (1), it follows that $S_{m+1}(n + 1) \equiv n + 1 \pmod{m}$. \square

Corollary 2.1. Let $n \geq 1$ be an integer. Then

$$S_{d+1}(n + 1) \equiv 1 \pmod{d}$$

for all divisors d of n .

Proof. Let d be a divisor of n . By Lemma 2.1, $S_{d+1}(n + 1) \equiv n + 1 \pmod{d}$, we have $S_{d+1}(n + 1) \equiv 1 \pmod{d}$. \square

3. LUCAS-CARMICHAEL INTEGERS

In this section, we prove a necessary and sufficient condition for Lucas-Carmichael integers and also prove a few interesting properties of such integers.

Proposition 3.1. *An integer $n > 1$ is a Lucas-Carmichael integer if and only if n is square-free and $S_{p+2}(n+2) \equiv 1 \pmod{p+1}$ for every prime divisor p of n . That is,*

$$\mathcal{L}_C = \left\{ n \in \mathcal{S} : p \mid n \implies S_{p+2}(n+2) \equiv 1 \pmod{p+1} \right\}.$$

Here, \mathcal{L}_C and \mathcal{S} denote the set of all Lucas-Carmichael integers and positive square-free integers, respectively.

Proof. Let $n > 1$ be a Lucas-Carmichael integer. Clearly, n is square-free, and by Corollary 2.1, $S_{p+2}(n+2) \equiv 1 \pmod{p+1}$ whenever p divides n .

Now, we prove the converse part. Assume that n is a square-free integer satisfying

$$S_{p+2}(n+2) \equiv 1 \pmod{p+1} \quad (2)$$

for all prime divisors p of n .

By Lemma 2.1, we have

$$S_{p+2}(n+2) \equiv n+2 \pmod{p+1}. \quad (3)$$

Combining equations (2) and (3), it is clear that $p+1$ divides $n+1$ whenever p divides n . \square

Proposition 3.2. *Every Lucas-Carmichael integer n is odd with at least three prime factors, and $p+1 \mid \frac{n}{p} - 1$ for every prime p divides n .*

Proof. Since $p+1$ divides $n+1$, $n+1$ is even, and thus n is odd.

Suppose that there is a Lucas-Carmichael integer n with exactly two prime factors p and q . Assume that $p > q$.

Since $p+1$ divides $n+1$, let

$$k := \frac{n+1}{p+1} = \frac{pq+1}{p+1} \in \mathbb{N}.$$

Then,

$$\begin{aligned} k &= \frac{pq - p + p + 1}{p + 1} \\ &= \frac{p(q - 1) + (p + 1)}{p + 1} \\ &= \frac{p(q - 1)}{p + 1} + 1. \end{aligned}$$

This implies that $p + 1$ divides $q - 1$, but it is not possible. Hence, n has at least three prime factors.

Now, we prove that $p + 1 \mid \frac{n}{p} - 1$ for every prime p divides n . Let $n = p_1 p_2 \cdots p_r$, $r \geq 3$ be a Lucas-Carmichael integer. Since $p_i + 1$ divides $n + 1$ for all i ,

$$k_i := \frac{n + 1}{p_i + 1} = \frac{p_1 p_2 \cdots p_r + 1}{p_i + 1} \in \mathbb{N}.$$

Let $n_i = \frac{n}{p_i}$ and we write

$$\begin{aligned} k_i &= \frac{p_1 p_2 \cdots p_r + n_i - n_i + 1}{p_i + 1} \\ &= \frac{n_i(p_i + 1) - (n_i - 1)}{p_i + 1} \\ &= n_i - \frac{(n_i - 1)}{p_i + 1}. \end{aligned}$$

Therefore, $\frac{(n_i - 1)}{p_i + 1} = n_i - k_i \in \mathbb{Z}$. That is, $p_i + 1$ divides $n_i - 1$. This completes the proof. \square

Corollary 3.1. Every prime factor p of a Lucas-Carmichael integer n is strictly less than \sqrt{n} .

Proof. By Proposition 3.2, we have $p < \frac{n}{p}$ for every prime factor p of n . This implies that $p < \sqrt{n}$. \square

Proposition 3.3. If $n = mqr$ is a Lucas-Carmichael integer where $m \in \mathbb{N}$ and q, r are primes with $q < r$. Then $q < 3m^2$ and $r < 3m^3$.

Proof. Since q and r are prime divisors of a Lucas-Carmichael integer n , we have $q + 1 \mid n + 1$ and $r + 1 \mid n + 1$.

That is,

$$mqr \equiv -mr \equiv -1 \pmod{q + 1} \text{ and } mqr \equiv -mq \equiv -1 \pmod{r + 1}.$$

Now, we define

$$C = \frac{mq - 1}{r + 1} \text{ and } D = \frac{mr - 1}{q + 1}.$$

Since $mq - 1 < mr - 1 < mr + m$, we have $C < m$.

As $r - q \geq 1$, we have $m - 1 < m \leq m(r - q)$. This implies that $m + mq < mr + 1$. Then

$$\begin{aligned} mq + m - q - 1 &< mr + 1 - q - 1 \\ m(q + 1) - (q + 1) &= mr - q < mr - 1 \\ (m - 1)(q + 1) &< mr - 1 \\ m - 1 &< \frac{mr - 1}{q + 1} = D. \end{aligned}$$

Therefore, we have $1 \leq C < m \leq D$. Now we consider:

$$\begin{aligned}
D(q+1) &= mr - 1 \\
&= m\left(\frac{mq-1}{C} - 1\right) - 1 \\
&= \frac{m^2q - m - mC - C}{C} \\
CD(q+1) &= m^2q - m - mC - C \\
&= m^2q + m^2 - m^2 - m - mC - C \\
(CD - m^2)(q+1) &= -m^2 - m - mC - C < 0.
\end{aligned}$$

This implies that,

$$\begin{aligned}
0 &< (m^2 - CD)(q+1) = m^2 + m + mC + C \\
q+1 &\leq m^2 + m(C+1) + C.
\end{aligned}$$

Since $C < m$, we obtain that $q+1 < m^2 + m^2 + m < 3m^2$ and hence $q < 3m^2$.

Next, we prove the other inequality. Consider,

$$r+1 = \frac{mq-1}{C} < \frac{m(q+1)}{C} < \frac{m(3m^2)}{C} < 3m^3.$$

and hence the inequality $r < 3m^3$ holds. \square

In the following section, we explicitly describe a class of Lucas-Carmichael integers.

4. SOME GENERAL FORMS OF LUCAS-CARMICHAEL INTEGERS

Recall that, from Proposition 3.1, an integer n is a Lucas-Carmichael integer if and only if $p+1$ divides $S_{p+2}(n+2)-1$ whenever p divides n . In this section, we study some general forms of Lucas-Carmichael integers with an odd number of prime factors. Also, we define the degree of a Lucas-Carmichael integer and prove some interesting results on the degree of such integers.

Definition 4.1. An integer $n \in \mathcal{L}_C$ is called a primary Lucas-Carmichael integer if $S_{p+2}(n+2) = p+2$ for every prime p divides n , and the set of all such integers is denoted by \mathcal{L}_C' .

Definition 4.2. Let n be a Lucas-Carmichael integer and

$$\alpha := \max_{p|n} \left\{ \frac{S_{p+2}(n+2) - 1}{p+1} \right\}.$$

The integer α is called the degree of n .

We note that primary Lucas-Carmichael integers have a degree of 1.

Now, we prove that there are infinitely many Lucas-Carmichael integers assuming the prime k -tuples conjecture (defined below).

The Prime k -tuples Conjecture. Let a_1, \dots, a_k be positive integers, and let b_1, \dots, b_k be nonzero integers. For $m \geq 1$, define $f(m) = \prod_{i=1}^k (a_i m + b_i)$. Let $P(x)$ denote the number of positive integers $m \leq x$ for which $a_i m + b_i$ is prime for each $i = 1, \dots, k$. The Prime k -tuples Conjecture states that if no prime divides $f(m)$ for every m , then there exists $c > 0$ such that $P(x) \sim \frac{cx}{\log^k x}$ as $x \rightarrow \infty$.

Chernick [5] called polynomial of the form $f(m)$ is universal if it satisfies the congruence relations $f(m) \equiv 1 \pmod{a_i m + b_i - 1}$ for every $i = 1, 2, \dots, k$, where $m \in \mathbb{Z}$, $k \geq 3$ and k is odd. Further, Chernick [5] proved that for any integers $k \geq 4$ and $m \geq 1$ such that 2^{k-4} divides m ,

$$U_k(m) = (6m + 1)(12m + 1) \prod_{i=1}^{k-2} (9 \cdot 2^i m + 1)$$

is a Carmichael number if each of the k factors is prime. We call $U_k(m)$ a Chernick polynomial.

Lemma 4.1. Let m be a positive integer, and $p = 6m - 1$, $q = 12m - 1$, $r = 18m - 1$ and $U'_3(m) = n = pqr$. Then

$$\begin{aligned} n + 2 &= 5(p + 2)^3 + (p - 27)(p + 2)^2 + 45(p + 2) + (p - 20) \\ n + 2 &= (9m - 5)(q + 2)^2 + (9m + 11)(q + 2) + (6m - 5) \\ n + 2 &= (4m - 2)(r + 2)^2 + (6m + 5)(r + 2) + (8m - 2). \end{aligned}$$

Proof. We rewrite $n + 2$ with the base $p + 2$ as follows:

$$\begin{aligned} n + 2 &= (216m^2 - 102m + 23)(p + 2) - 22 \\ &= (36m - 23)(p + 2)^2 + 46(p + 2) - 22 \\ &= 5(p + 2)^3 + (p - 27)(p + 2)^2 + 46(p + 2) - 22 \\ &= 5(p + 2)^3 + (p - 27)(p + 2)^2 + 45(p + 2) + (p - 20). \end{aligned}$$

Similarly, we can write $n + 2$ with the base $q + 2$ as follows:

$$\begin{aligned} n + 2 &= (108m^2 - 42m)(q + 2) + (78m + 1) \\ &= 9m(q + 2)^2 - 5(q + 2)^2 + (9m + 11)(q + 2) + (6m - 5) \\ &= (9m - 5)(q + 2)^2 + (9m + 11)(q + 2) + (6m - 5). \end{aligned}$$

Next, we can also write $n + 2$ with the base $r + 2$ as follows:

$$\begin{aligned} n + 2 &= (72m^2 - 26m)(r + 2) + (62m + 1) \\ &= 4m(r + 2)^2 - 2(r + 2)^2 + (6m + 5)(r + 2) + (8m - 2) \\ &= (4m - 2)(r + 2)^2 + (6m + 5)(r + 2) + (8m - 2). \end{aligned}$$

□

Corollary 4.1. Assuming the same hypotheses as Lemma 4.1 with $m \geq 8$, we have $S_{p+2}(n+2) = 2p+3$, $S_{q+2}(n+2) = 2q+3$ and $S_{r+2}(n+2) = r+2$.

Proof. Since $p \geq 47$ as $m \geq 8$, the coefficients of $n+2$ in the first equation in Lemma 4.1 are lie between 0 and $p+1$, so we have $n+2$ with base $p+2$. Thus, $S_{p+2}(n+2) = 5+(p-27)+45+(p-20) = 2p+3$.

Similarly, the coefficients of $n+2 = (9m-5)(q+2)^2 + (9m+11)(q+2) + (6m-5)$ are between 0 and $q+1$, we have $S_{q+2}(n+2) = (9m-5) + (9m+11) + (6m-5) = 24m+1 = 2q+3$.

Also, the coefficients of $n+2 = (4m-2)(r+2)^2 + (6m+5)(r+2) + (8m-2)$ are between 0 and $r+1$, we have $S_{r+2}(n+2) = (4m-2) + (6m+5) + (8m-2) = 18m+1 = r+2$. □

Theorem 4.1. The prime k -tuples conjecture implies that there are infinitely many Lucas-Carmichael integers of degree 2 with exactly three prime factors.

Proof. By the prime k -tuples conjecture, there are infinitely many positive integers m such that $U'_3(m)$ has three distinct prime factors. Applying the Corollary 4.1, each of these numbers $U'_3(m)$ for $m \geq 8$ is a Lucas-Carmichael integer of degree 2. □

Theorem 4.2. Every Lucas-Carmichael integer n with exactly three prime factors is of the form $(2hr_1-1)(2hr_2-1)(2hr_3-1)$, where h is a positive integer and r_i 's are pairwise co-prime integers.

Proof. Let $n = p_1p_2p_3$ be a Lucas-Carmichael integer with three prime factors. Write $p_i = r_i k - 1$, where k is the *g.c.d.* of $p_i + 1$ for $i = 1, 2, 3$. Since n is a Lucas-Carmichael integer, we have

$$(r_1 k - 1)(r_2 k - 1)(r_3 k - 1) \equiv -1 \pmod{p_i + 1}$$

for $i = 1, 2, 3$. This implies that,

$$(r_1 r_2 r_3) k^3 - (r_1 r_2 + r_1 r_3 + r_2 r_3) k^2 + (r_1 + r_2 + r_3) k - 1 \equiv -1 \pmod{r_i k}.$$

By simplifying the above congruence, we obtain

$$-(r_1 r_2 + r_1 r_3 + r_2 r_3) k + (r_1 + r_2 + r_3) \equiv 0 \pmod{r_i}.$$

For $1 \leq i \neq j \leq 3$, if r_i and r_j have a common factor, then the third one does, and it contradicts our assumption. Hence, the r_i 's are pairwise co-prime. Suppose k is odd, then r_i 's are even as p_i 's are odd. Since k is the *g.c.d.* of $p_i + 1$, this is not possible. Therefore, k must be even, and the theorem follows. □

Theorem 4.3. Let F'_l be a Lucas-Carmichael integer with exactly l -odd number of prime factors p_1, p_2, \dots, p_l . Let k_1 be the *g.c.d.* of $p_i + 1$ and $r_i = \frac{p_i + 1}{k_1}$. Also, let R be the *l.c.m.* of r_i , $i = 1, 2, \dots, l$. Then $U'_l(m) = \prod_{i=1}^l (r_i R m + p_i)$ satisfies the congruence relation

$$U'_l(m) \equiv -1 \pmod{r_i R m + p_i + 1}$$

for $i = 1, 2, \dots, l$.

Proof. Since $F'_l = \prod_{i=1}^l (r_i k_1 - 1)$ is a Lucas-Carmichael integer and l is odd, we have $\prod_{i=1}^l (r_i k_1 - 1) \equiv -1 \pmod{r_i k_1}$ for $i = 1, 2, \dots, l$.

This implies that

$$\frac{\prod_{i=1}^l (r_i k_1 - 1) + 1}{k_1} \equiv 0 \pmod{r_i}$$

for $i = 1, 2, \dots, l$.

Therefore,

$$\frac{\prod_{i=1}^l (r_i k_1 - 1) + 1}{k_1} \equiv 0 \pmod{R}.$$

We observe that, any $k \equiv k_1 \pmod{R}$ is also a solution for the above congruence. Write $k = Rm + k_1$ and substitute this k for k_1 , we obtain

$$\frac{\prod_{i=1}^l (r_i (Rm + k_1) - 1) + 1}{k} \equiv 0 \pmod{R}.$$

Since $p_i = r_i k - 1$ and $r_i k = r_i R m + r_i k_1 = r_i R m + p_i + 1$, we have

$$\prod_{i=1}^l (r_i R m + p_i) + 1 \equiv 0 \pmod{r_i k}$$

and

$$U'_l(m) = \prod_{i=1}^l (r_i R m + p_i) \equiv -1 \pmod{r_i R m + p_i + 1}$$

for every i ranges over 1 to l . \square

Remark: Since $U'_l(m) = \prod_{i=1}^l (r_i R m + p_i)$ satisfies the congruence relation

$$U'_l(m) \equiv -1 \pmod{r_i R m + p_i + 1}$$

for $i = 1, 2, \dots, l$, the integer $U'_l(m)$ is a Lucas-Carmichael integer for every m for which each of the l factors is a prime.

We illustrate Theorem 4.3 with the examples below.

Example 4.1. Let $F'_5 = 588455$ be a Lucas-Carmichael integer. Then, we have $k_1 = 2$, $r_1 = 3$, $r_2 = 4$, $r_3 = 9$, $r_4 = 12$, $r_5 = 22$ and $R = 396$. Let $U'_5(m) = n = p_1 p_2 p_3 p_4 p_5$, where $p_1 = 1188m + 5$, $p_2 = 1584m + 7$, $p_3 = 3564m + 17$, $p_4 = 4752m + 23$ and $p_5 = 8712m + 43$. Then, by Theorem 4.3, we have $U'_5(m) \equiv -1 \pmod{396r_i + p_i + 1}$ for every $i = 1, 2, 3, 4, 5$.

Now, we prove that there are infinitely many Lucas-Carmichael integers of degree 4 with exactly five prime factors.

Lemma 4.2. Let m be a positive integer, and $p = 1188m + 5$, $q = 1584m + 7$, $r = 3564m + 17$, $s = 4752m + 23$, $t = 8712m + 43$ and $U'_5(m) = n = pqrst$. Then

$$\begin{aligned}
n + 2 &= 117(p + 2)^5 + (396m - 875)(p + 2)^4 + (1056m + 2593)(p + 2)^3 \\
&\quad + (660m - 3771)(p + 2)^2 + (132m + 2724)(p + 2) + (132m - 775) \\
n + 2 &= 27(q + 2)^5 + \left(\frac{2117016}{1584}m - 224\right)(q + 2)^4 \\
&\quad + \left(\frac{1724976}{1584}m + 758\right)(q + 2)^3 + \left(\frac{2273832}{1584}m - 1199\right)(q + 2)^2 \\
&\quad + (1287m + 958)(q + 2) + (1188m - 287) \\
n + 2 &= \left(\frac{6133248}{3564}m + 3\right)(r + 2)^4 + \left(\frac{2317392}{3564}m + 32\right)(r + 2)^3 \\
&\quad + \left(\frac{574992}{3564}m - 65\right)(r + 2)^2 + \left(\frac{4373424}{3564}m + 78\right)(r + 2) \\
&\quad + \left(\frac{12005136}{3564}m - 11\right) \\
n + 2 &= \left(\frac{2587464}{4752}m + 1\right)(s + 2)^4 + \left(\frac{3606768}{4752}m + 13\right)(s + 2)^3 \\
&\quad + \left(\frac{14662296}{4752}m - 10\right)(s + 2)^2 + (1023m + 38)(s + 2) \\
&\quad + (4092m + 7) \\
n + 2 &= \left(\frac{419904}{8712}m\right)(t + 2)^4 + \left(\frac{9191232}{8712}m + 6\right)(t + 2)^3 \\
&\quad + \left(\frac{41885424}{8712}m + 20\right)(t + 2)^2 + \left(\frac{31403376}{8712}m + 26\right)(t + 2) \\
&\quad + \left(\frac{68897952}{8712}m + 37\right).
\end{aligned}$$

Corollary 4.2. Assume that the same hypotheses in Lemma 4.2 with $156816 \mid m$. Then, we have $S_{p+2}(n + 2) = 2p + 3$, $S_{q+2}(n + 2) = 4q + 5$, $S_{r+2}(n + 2) = 2r + 3$, $S_{s+2}(n + 2) = 2s + 3$ and $S_{t+2}(n + 2) = 2t + 3$.

Theorem 4.4. The prime k -tuples conjecture implies that there are infinitely many Lucas-Carmichael integers of degree 4 with exactly five prime factors.

Proof. From the prime k -tuples conjecture, we have infinitely many positive integers m which are divisible by 156816, and $U_5'(m)$ has exactly five prime factors. By Corollary 4.2, each of these numbers $U_5'(m)$ is a Lucas-Carmichael integer of degree 4. \square

Example 4.2. Let $F_7' = 3512071871$ be a Lucas-Carmichael integer. Then, we have $k_1 = 2, r_1 = 4, r_2 = 6, r_3 = 9, r_4 = 12, r_5 = 16, r_6 = 27, r_7 = 36$ and $R = 432$. Let $U_7'(m) = p_1 p_2 p_3 p_4 p_5 p_6 p_7$, where $p_1 = 1728m + 7, p_2 = 2592m + 11, p_3 = 3888m + 17, p_4 = 5184m + 23, p_5 = 6912m + 31, p_6 = 11664m + 53, p_7 = 15552m + 71$ and $U_7'(m) = n = p_1 p_2 p_3 p_4 p_5 p_6 p_7$. Then, by Theorem 4.3, we have $U_7'(m) \equiv -1 \pmod{432r_i + p_i + 1}$ for every $i = 1, 2, 3, 4, 5, 6, 7$.

Next, we prove that there are infinitely many Lucas-Carmichael integers of degree 4 with exactly seven prime factors.

Lemma 4.3. Let m be a positive integer, and $p = 1728m + 7, q = 2592m + 11, r = 3888m + 17, s = 5184m + 23, t = 6912m + 31, u = 11664m + 53, v = 15552m + 71$ and $U_7'(m) = n = pqrstuv$. Then

$$\begin{aligned}
n + 2 &= 2460(p + 2)^7 + (648m - 24487)(p + 2)^6 \\
&\quad + (918m + 103732)(p + 2)^5 + (1512m - 242426)(p + 2)^4 \\
&\quad + (1026m + 337790)(p + 2)^3 + (432m - 280653)(p + 2)^2 \\
&\quad + (1512m + 128798)(p + 2) + (864m - 25181) \\
n + 2 &= 143(q + 2)^7 + (2592m - 1644)(q + 2)^6 + 7965(q + 2)^5 \\
&\quad + (1728m - 21163)(q + 2)^4 + (720m + 33401)(q + 2)^3 \\
&\quad + (216m - 31287)(q + 2)^2 + (2088m + 16136)(q + 2) \\
&\quad + (432m - 3525) \\
n + 2 &= 8(r + 2)^7 + (1664m - 107)(r + 2)^6 + \left(\frac{1456}{3}m + 662\right)(r + 2)^5 \\
&\quad + \left(\frac{944}{3}m - 2064\right)(r + 2)^4 + \left(\frac{11152}{3}m + 3829\right)(r + 2)^3 \\
&\quad + \left(\frac{3776}{3}m - 4148\right)(r + 2)^2 + \left(\frac{3376}{3}m + 2482\right)(r + 2) \\
&\quad + \left(\frac{9296}{3}m - 607\right)
\end{aligned}$$

$$\begin{aligned}
n + 2 &= (s + 2)^7 + (648m - 15)(s + 2)^6 + (1458m + 125)(s + 2)^5 \\
&\quad + (1404m - 419)(s + 2)^4 + (4086m + 915)(s + 2)^3 \\
&\quad + (4212m - 1090)(s + 2)^2 + (2016m + 758)(s + 2) \\
&\quad + (1728m - 202)
\end{aligned}$$

$$\begin{aligned}
n + 2 &= \left(\frac{531441}{512}m + 2\right)(t + 2)^6 + \left(\frac{460701}{512}m + 26\right)(t + 2)^5 \\
&\quad + \left(\frac{312795}{128}m - 82\right)(t + 2)^4 + \left(\frac{1532709}{256}m + 256\right)(t + 2)^3 \\
&\quad + \left(\frac{811161}{512}m - 319\right)(t + 2)^2 + \left(\frac{1590921}{512}m + 267\right)(t + 2) \\
&\quad + \left(\frac{1453005}{256}m - 53\right)
\end{aligned}$$

$$\begin{aligned}
n + 2 &= \left(\frac{32768}{729}m\right)(u + 2)^6 + \left(\frac{919552}{729}m + 7\right)(u + 2)^5 \\
&\quad + \left(\frac{793744}{729}m - 2\right)(u + 2)^4 + \left(\frac{1154864}{243}m + 45\right)(u + 2)^3 \\
&\quad + \left(\frac{1404608}{729}m - 36\right)(u + 2)^2 + \left(\frac{5584880}{729}m + 82\right)(u + 2) \\
&\quad + \left(\frac{4805968}{729}m + 13\right)
\end{aligned}$$

$$\begin{aligned}
n + 2 &= 8m(v + 2)^6 + \left(\frac{946}{3}m + 1\right)(v + 2)^5 + \left(\frac{33416}{3}m + 50\right)(v + 2)^4 \\
&\quad + \left(\frac{26998}{3}m + 49\right)(v + 2)^3 + \left(\frac{13664}{3}m + 4\right)(v + 2)^2 \\
&\quad + \left(\frac{31096}{3}m + 69\right)(v + 2) + \left(\frac{33824}{3}m + 44\right).
\end{aligned}$$

Corollary 4.3. Assume that the same hypotheses in Lemma 4.3 with $373248 \mid m$. Then, we have $S_{p+2}(n + 2) = 4p + 5$, $S_{q+2}(n + 2) = 3q + 4$, $S_{r+2}(n + 2) = 3r + 4$, $S_{s+2}(n + 2) = 3s + 4$, $S_{t+2}(n + 2) = 3t + 4$, $S_{u+2}(n + 2) = 2u + 3$ and $S_{v+2}(n + 2) = 3v + 4$.

Theorem 4.5. The prime k -tuples conjecture implies that there are infinitely many Lucas-Carmichael integers of degree 4 with exactly seven prime factors.

Proof. According to the prime k -tuples conjecture, there are infinitely many positive integers m divisible by 373248 for which $U_7^l(m)$ has exactly seven prime factors. By Corollary 4.3, each of these numbers $U_7^l(m)$ is a Lucas-Carmichael integer of degree 4. \square

Acknowledgements. The second author would like to acknowledge support from MeitY QCAL. Also, the second author would like to acknowledge support from ICTP through the associate programme.

REFERENCES

- [1] Samuel S. Wagstaff, Jr. *Primary Carmichael Numbers*, Integers, 22 (2022).
- [2] R. D. Carmichael, *Note on a new number theory function*, Bull. Amer. Math. Soc. 16 (1910), 232-238.
- [3] R. D. Carmichael, *On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \pmod{P}$* , Amer. Math. Monthly 19 (1912), 22-27.
- [4] A. Korselt, *Problème chinois*, L'Intermédiaire Math. 6 (1899), 142-143.
- [5] J. Chernick, *On Fermat's simple theorem*, Bull. Amer. Math. Soc. 45 (1939), 269-274.
- [6] W. R. Alford, A. Granville, and C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. (2), 139 (3) (1994), 703-722.
- [7] B. C. Kellner and J. Sondow, *On Carmichael and polygonal numbers, Bernoulli polynomials, and sums of base- p digits*, Integers 21 (2021), #A52, 1-21.
- [8] Thomas Wright, *There are infinitely many elliptic Carmichael numbers*, Bulletin of the London Mathematical Society, 50 (2018), 791-800.
- [9] D. M. Gordon, *Pseudoprimes on elliptic curves*, Théorie des nombres (Quebec, PQ, 1987), (1989), 290-305.
- [10] A. Ekstrom, C. Pomerance and D. S. Thakur, *Infinitude of elliptic Carmichael numbers*, J. Aust. Math. Soc. 92 (2012), 45-60.

⁽¹⁾ INDIAN INSTITUTE OF INFORMATION TECHNOLOGY, DESIGN AND MANUFACTURING, KANCHEEPURAM, CHENNAI - 600127, INDIA

⁽²⁾ INDIAN INSTITUTE OF INFORMATION TECHNOLOGY, DESIGN AND MANUFACTURING, KANCHEEPURAM, CHENNAI - 600127, INDIA

Email address: ⁽¹⁾mat20d001@iiitdm.ac.in

Email address: ⁽²⁾subramani@iiitdm.ac.in