ON K-LEHMER NUMBERS

José María Grau
Departmento de Matemáticas, Universidad de Oviedo, Oviedo, Spain
grau@uniovi.es

Antonio M. Oller-Marcén
Centro Universitario de la Defensa, Academia General Militar, Zaragoza, Spain
oller@unizar.es

Received: 10/27/11, Revised: 2/21/12, Accepted: 5/22/12, Published: 6/25/12

Abstract

Lehmer's totient problem consists of determining the set of positive integers n such that $\varphi(n) \mid (n-1)$ where φ is Euler's totient function. In this paper we introduce the concept of k-Lehmer number. A k-Lehmer number is a composite number such that $\varphi(n) \mid (n-1)^k$. The relation between k-Lehmer numbers and Carmichael numbers leads to a new characterization of Carmichael numbers and to some conjectures related to the distribution of Carmichael numbers which are also k-Lehmer numbers.

1. Introduction

Lehmer's totient problem asks about the existence of a composite number such that $\varphi(n) \mid (n-1)$, where φ is Euler's totient function. Some authors refer to these numbers as *Lehmer numbers*. In 1932, Lehmer [14] showed that every Lehmer number n must be odd and square-free, and that the number of distinct prime factors of n, $\omega(n)$, must satisfy $\omega(n) > 6$. This bound was subsequently extended to $\omega(n) > 10$. The current best result, due to Cohen and Hagis [10], is that n must have at least 14 prime factors and the biggest lower bound obtained for such numbers is 10^{30} [18]. It is known that there are no Lehmer numbers in certain sets, such as the Fibonacci sequence [16], the sequence of repunits in base g for any $g \in [2, 1000]$ [9] or the Cullen numbers [12]. In fact, no Lehmer numbers are known up to date. For further results on this topic we refer the reader to [4, 5, 17, 19].

A *Carmichael number* is a composite positive integer n satisfying the congruence $b^{n-1} \equiv 1 \pmod{n}$ for every integer b relatively prime to n. Korselt [13] was the first to observe the basic properties of Carmichael numbers, the most important being the following characterization:

Proposition 1. (Korselt, 1899) *A composite number n is a Carmichael number if and only if n is square-free, and for each prime p dividing n, $p-1$ divides $n-1$.*

Nevertheless, Korselt did not find any example and it was Robert Carmichael in 1910 [7] who found the first and smallest of such numbers (561) and hence the name "Carmichael number" (which was introduced by Beeger [6]). In the same paper Carmichael presents a function λ defined in the following way:

- $\lambda(2) = 1$, $\lambda(4) = 2$.
- $\lambda(2^k) = 2^{k-2}$ for every $k \geq 3$.
- $\lambda(p^k) = \varphi(p^k)$ for every odd prime p.
- $\lambda(p_1^{k_1} \cdots p_m^{k_m}) = \operatorname{lcm}\Big(\lambda(p_1^{k_1}), \ldots, \lambda(p_m^{k_m})\Big)$.

With this function he gave the following characterization:

Proposition 2. (Carmichael, 1910) *A composite number n is a Carmichael number if and only if $\lambda(n)$ divides $(n-1)$.*

In 1994 Alford, Granville and Pomerance [1] answered in the affirmative the long-standing question whether there were infinitely many Carmichael numbers. From a more computational viewpoint, an algorithm to construct large Carmichael numbers has been given [15]. Also the distribution of certain types of Carmichael numbers is studied [3].

In this work we introduce the condition $\varphi(n) \mid (n-1)^k$ (that we shall call *k-Lehmer property* and the associated concept of k-Lehmer numbers. In Section 2 we give some properties of the sets L_k (the set of numbers satisfying the k-Lehmer property) and $L_\infty := \bigcup_{k\geq 1} L_k$, characterizing this latter set. In Section 3 we show that every Carmichael number is also a k-Lehmer number for some k. Finally, in Section 4 we use Chernick's formula to construct Camichael numbers in $L_k \setminus L_{k-1}$ and we give some related conjectures.

2. A Generalization of Lehmer's Totient Property

Recall that a *Lehmer number* is a composite integer n such that $\varphi(n) \mid (n-1)$. Following this idea we present the definition below.

Definition 3. Given $k \in \mathbb{N}$, a k-Lehmer number is a composite integer n such that $\varphi(n) \mid (n-1)^k$. If we denote by L_k the set:

$$L_k := \{n \in \mathbb{N} \ : \ \varphi(n) \mid (n-1)^k\},$$

it is clear that k-Lehmer numbers are the composite elements of L_k.

Once we have defined the family of sets $\{L_k\}_{k\geq 1}$ and since $L_k \subseteq L_{k+1}$ for every k, it makes sense to define a set L_∞ in the following way:

$$L_\infty := \bigcup_{k=1}^{\infty} L_k.$$

The set L_∞ is easily characterized in the following proposition.

Proposition 4. *The set L_∞ defined above admits the following characterization:*

$$L_\infty = \{n \in \mathbb{N} \ : \ rad(\varphi(n)) \mid (n-1)\}.$$

Proof. Let $n \in L_\infty$. Then $n \in L_k$ for some $k \in \mathbb{N}$. Now, if p is a prime dividing $\varphi(n)$, it follows that p divides $(n-1)^k$ and, being prime, it also divides $n-1$. This proves that $\mathrm{rad}(\varphi(n)) \mid (n-1)$.

On the other hand, if $\mathrm{rad}(\varphi(n)) \mid (n-1)$ it is clear that $\varphi(n) \mid (n-1)^k$ for some $k \in \mathbb{N}$. Thus $n \in L_k \subseteq L_\infty$ and the proof is complete. □

Obviously, the composite elements of L_1 are precisely the Lehmer numbers and the Lehmer property asks whether L_1 contains composite numbers or not. Nevertheless, for all $k > 1$, L_k always contains composite elements. For instance, the first few composite elements of L_2 are (sequence A173703 in OEIS):

$$\{561, 1105, 1729, 2465, 6601, 8481, 12801, 15841, 16705, 19345, 22321, 30889, 41041, \dots\}.$$

Observe that in the previous list of elements of L_2 there are no products of two distinct primes. We will now prove this fact, which is also true for Carmichael numbers. Observe that this property is no longer true for L_3 since, for instance, $15 \in L_3$ and also the product of two Fermat primes lies in L_∞.

In order to show that no product of two distinct odd primes lies in L_2 we will give a stronger result which determines when an integer of the form $n = pq$ (with $p \neq q$ odd primes) lies in a given L_k.

Proposition 5. *Let p and q be distinct odd primes and let $k \geq 2$. Put $p = 2^a d\alpha + 1$ and $q = 2^b d\beta + 1$ with d, α, β odd and $\gcd(\alpha, \beta) = 1$. We can assume without loss of generality that $a \leq b$. Then $n = pq \in L_k$ if and only if $a + b \leq ka$ and $\alpha\beta \mid d^{k-2}$.*

Proof. By definition $pq \in L_k$ if and only if $\varphi(pq) = (p-1)(q-1) = 2^{a+b}d^2\alpha\beta$ divides $(pq-1)^k = \left(2^{a+b}d^2\alpha\beta + 2^a d\alpha + 2^b d\beta\right)^k$. If we expand the latter using the multinomial theorem it easily follows that $pq \in L_k$ if and only if $2^{a+b}d^2\alpha\beta$ divides $2^{ka}d^k\alpha^k + 2^{kb}d^k\beta^k = 2^{ka}d^k\left(\alpha^k + 2^{k(b-a)}\beta^k\right)$.

Now, if $a \neq b$ observe that $\left(\alpha^k + 2^{k(b-a)}\beta^k\right)$ is odd and, since $\gcd(\alpha, \beta) = 1$, it follows that $\gcd(\alpha, \alpha^k + 2^{k(b-a)}\beta^k) = \gcd(\beta, \alpha^k + 2^{k(b-a)}\beta^k) = 1$. This implies that $pq \in L_k$ if and only if $a + b \leq ka$ and $\alpha\beta$ divides d^{k-2}, as claimed.

If $a = b$ then $pq \in L_k$ if and only if $\alpha\beta$ divides $d^{k-2}\left(\alpha^k + \beta^k\right)$ and the result follows as in the previous case. Observe that in this case the condition $a + b \leq ka$ is vacuous since $k \geq 2$. □

Corollary 6. *If p and q are distinct odd primes, then $pq \notin L_2$.*

Proof. By the previous proposition and using the same notation, $pq \in L_2$ if and only if $a + b \leq 2a$ and $\alpha\beta$ divides 1. Since $a \leq b$ the first condition implies that $a = b$ and the second condition implies that $\alpha = \beta = 1$. Consequently $p = q$, a contradiction. □

It would be interesting to find an algorithm to construct elements in a given L_k. The easiest step in this direction, using similar ideas to those in Proposition 6, is given in the following result.

Proposition 7. *Let $p_r = 2^r \cdot 3 + 1$. If p_N and p_M are primes and $M - N$ is odd, then $n = p_N p_M \in L_K$ for $K = \min\{k \ : \ kN \geq M + N\}$ and $n \notin L_{K-1}$.*

We will end this section with a table showing some values of the counting function for some L_k. If

$$C_k(x) := \sharp\{n \in L_k : n \leq x\},$$

we have the following data:

n	1	2	3	4	5	6	7	8
$C_2(10^n)$	5	26	170	1236	9613	78535	664667	5761621
$C_3(10^n)$	5	29	179	1266	9714	78841	665538	5763967
$C_4(10^n)$	5	29	182	1281	9784	79077	666390	5766571
$C_5(10^n)$	5	30	184	1303	9861	79346	667282	5769413
$C_\infty(10^n)$	5	30	188	1333	10015	80058	670225	5780785

In the light of the table above, it seems that the asymptotic behavior of C_k does not depend on k. It is also reasonable to think that the relative asymptotic density of the set of prime numbers in L_k is zero and that the relative asymptotic density of L_k in the set of cyclic numbers (see Lemma 9 below) is zero in turn. These ideas motivate the following conjecture:

Conjecture 8. The following hold:

i) $C_k(n) \approx C_\infty(n)$ for every $k \in \mathbb{N}$,

ii) $\displaystyle\lim_{n\to\infty} \frac{n}{C_\infty(n) \log\log\log n} = \infty$,

iii) $\displaystyle\lim_{n\to\infty} \frac{n}{C_\infty(n) \log n} = 0$,

iv) $C_\infty(n) \in \mathcal{O}\left(\dfrac{n}{\log\log n}\right)$.

3. Relation with Carmichael Numbers

This section will study the relation of L_∞ with square-free integers and with Carmichael numbers. The characterization of L_∞ given in Proposition 4 allows us to present the following straightforward lemma which, in particular, implies that L_∞ has zero asymptotic density (like the set of cyclic numbers, whose counting function is $\mathcal{O}\left(\frac{x}{\log\log\log x}\right)$ [11].

Lemma 9. *If $n \in L_\infty$, then n is a cyclic number; i.e.,* $\gcd(n, \varphi(n)) = 1$ *and consequently square-free.*

Recall that every Lehmer number (if any exists) must be a Carmichael number. The converse is clearly false but, nevertheless, we can see that every Carmichael number is a k-Lehmer number for some $k \in \mathbb{N}$.

Proposition 10. *If n is a Carmichael number, then $n \in L_\infty$*

Proof. Let n be a Carmichael number. By Korselt's criterion $n = p_1 \cdots p_m$ and $p_i - 1$ divides $n-1$ for every $i \in \{1, \ldots, m\}$. We have that $\varphi(n) = (p_1 - 1)\cdots(p_m - 1)$ and we can put $rad(\varphi(n)) = q_1 \cdots q_r$ with q_j distinct primes. Now let $j \in \{1, \ldots, r\}$; since q_j divides $\varphi(n)$ it follows that q_j divides $p_i - 1$ for some $i \in \{1, \ldots, m\}$ and also that q_j divides $n - 1$. This implies that $rad(\varphi(n))$ divides $n - 1$ and the result follows. □

The two previous results lead to a characterization of Carmichael numbers which slightly modifies Korselt's criterion. Namely, we have the following result.

Theorem 11. *A composite number n is a Carmichael number if and only if $rad(\varphi(n))$ divides $n - 1$, and $p - 1$ divides $n - 1$, for every prime divisor p of n.*

Proof. We have already seen in Proposition 10 that if n is a Carmichael number, then $rad(\varphi(n))$ divides $n-1$ and, by Korselt's criterion $p-1$ divides $n-1$ for every prime divisor p of n.

Conversely, if $rad(\varphi(n))$ divides $n-1$ then by Lemma 9 we have that n is square-free, so it is enough to apply Korselt's criterion again. □

The set L_∞ not only contains every Carmichael number (which are pseudoprimes to all bases). It is known that every odd composite n (with the exception of the powers fo 3) has the property that it is a pseudoprime to base b for some b in $[2, n-2]$. In fact there is a formula [2] for the total number of such bases. In our case the elements of L_∞ are pseudoprimes to many different bases. Some of them are explicitly described in the following proposition.

Proposition 12. *Let $n \in L_\infty$ be a composite integer and let b be an integer such that $b \equiv a^{\frac{\varphi(n)}{rad(\varphi(n))}} \pmod{n}$ for some a with* $\gcd(a, n) = 1$. *Then n is a Fermat pseudoprime to base b.*

Proof. Since $n \in L_\infty$, it is odd and $\text{rad}(\varphi(n))$ divides $n-1$. Thus: $b^{n-1} \equiv a^{\frac{\varphi(n)(n-1)}{\text{rad}(\varphi(n))}} = a^{\varphi(n)\frac{n-1}{\text{rad}(\varphi(n))}} \equiv 1 \pmod{n}$. □

4. Carmichael Numbers in $L_k \setminus L_{k-1}$. Some Conjectures.

Recall the list of elements from L_2 given in the previous section:

$\{\mathbf{561}, \mathbf{1105}, \mathbf{1729}, \mathbf{2465}, \mathbf{6601}, 8481, 12801, \mathbf{15841}, 16705, 19345, 22321, 30889, 41041 \dots\}$.

Here, numbers in boldface are Carmichael numbers. Observe that not every Carmichael number lies in L_2, the smallest absent one being 2821. Although 2821 doe not lie in L_2 in is easily seen that 2821 lies in L_3.

It would be interesting to study the way in that Carmichael numbers are distributed among the sets L_k. In this section we will present a first result in this direction together with some conjectures.

Recall Chernick's formula [8]:

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

$U_k(m)$ is a Carmichael number provided all the factors are prime and 2^{k-4} divides m. Whether this formula produces an infinity quantity of Carmichael numbers is still not known, but we will see that it behaves quite nicely with respect to our sets L_k.

Proposition 13. *Let $k > 2$. If $(6m+1)$, $(12m+1)$ and $(9 \cdot 2^i m+1)$ for $i = 1, \dots, k-2$ are primes and $m \equiv 0 \pmod{2^{k-4}}$ is not a power of 2, then $U_k(m) \in L_k \setminus L_{k-1}$.*

Proof. It can be easily seen by induction (we give no details) that

$$U_k(m) - 1 = 2^2 3^2 m \left(2^{k-3} + \sum_{i=1}^{k-1} a_i m^i\right).$$

On the other hand we have that

$$\varphi\left(U_k(m)\right) = 2^{\frac{k^2-3k+8}{2}} 3^{2k-2} m^k.$$

We now show that $U_k(m) \in L_k$. To do so we study two cases:

`Case 1.` $3 \le k \le 5$. In this case $\frac{k^2-3k+8}{2} < 2k$ and, consequently:

$$\varphi\left(U_k(m)\right) = 2^{\frac{k^2-3k+8}{2}} 3^{2k-2} m^k \mid (2^2 3^2 m)^k \mid (U_k(m)-1)^k.$$

`Case 2.` $k \ge 6$. Since 2^{k-4} divides m we have that 2^{k-4} divides $2^{k-3} + \sum_{i=1}^{k-1} a_i m^i$. Consequently, since $2k(k-4) \ge \frac{k^2-3k+8}{2}$ in this case, we get that:

$$\varphi\left(U_k(m)\right) = 2^{\frac{k^2-3k+8}{2}} 3^{2k-2} m^k \mid 2^{2k(k-4)} 3^{2k-2} m^k \mid (U_k(m)-1)^k.$$

Now, we will see that $U_k(m) \notin L_{k-1}$. Since

$$(U_k(m)-1)^{k-1} = 2^{2k-2}3^{2k-2}\left(2^{k-3}+\sum_{i=1}^{k-1} a_i m^i\right)^{k-1},$$

it follows that $U_k(m) \in L_{k-1}$ if and only if $2^{\frac{(k-3)(k-4)}{2}}m$ divides $\left(\sum_{i=1}^{k-1} a_i m^i\right)^{k-1}$. If we put $m = 2^h m'$ with m' odd this latter condition implies that $m' \mid 2^{k-3}k-1$ which is clearly a contradiction because m is not a power of 2. This ends the proof. □

This result motivates the following conjecture.

Conjecture 14. For every $k \in \mathbb{N}$, $L_{k+1} \setminus L_k$ contains infinitely many Carmichael numbers.

Now, given $k \in \mathbb{N}$, let us denote by $\alpha(k)$ the smallest Carmichael number n such that $n \notin L_k$:

$$\alpha(k) = \min\{n \ : \ n \text{ is a Carmichael number}, \ n \notin L_k\}.$$

The following table presents the first few elements of this sequence (A207080 in OEIS):

k	$\alpha(k)$	Prime Factors
1	561	3
2	2821	3
3	838201	4
4	41471521	5
5	45496270561	6
6	776388344641	7
7	344361421401361	8
8	375097930710820681	9
9	330019822807208371201	10

These observations motivate the following conjectures which close the paper:

Conjecture 15. For every $k \in \mathbb{N}$, $\alpha(k) \in L_{k+1}$.

Conjecture 16. For every $2 < k \in \mathbb{N}$, $\alpha(k)$ has $k+1$ prime factors.

Acknowledgements The authors wish to thank the referee for his useful comments that have helped us to improve the paper.

References

[1] W.R. Alford, A. Granville, and C. Pomerance. There are infinitely many Carmichael numbers. *Ann. of Math. (2)*, 139(3):703–722, 1994.

[2] R. Baillie and S.S. Wagstaff, Jr. Lucas pseudoprimes. *Math. Comp.*, 35(152):1391–1417, 1980.

[3] R. Balasubramanian and S.V. Nagaraj. Density of Carmichael numbers with three prime factors. *Math. Comp.*, 66(220):1705–1708, 1997.

[4] W.D. Banks, A.M. Güloğlu, and C.W. Nevans. On the congruence $N \equiv A \pmod{\phi(N)}$. *Integers*, 8:A59, 8, 2008.

[5] W.D. Banks and F. Luca. Composite integers n for which $\phi(n) \mid n-1$. *Acta Math. Sin. (Engl. Ser.)*, 23(10):1915–1918, 2007.

[6] N.G.W.H. Beeger. On composite numbers n for which $a^{n-1} \equiv (\bmod\, n)$ for every a prime to n. *Scripta Math.*, 16:133–135, 1950.

[7] R.D. Carmichael. Note on a new number theory function. *Bull. Amer. Math. Soc.*, 16(5):232–238, 1910.

[8] J. Chernick. On Fermat's simple theorem. *Bull. Amer. Math. Soc.*, 45(4):269–274, 1939.

[9] J. Cilleruelo and F. Luca. Repunit Lehmer numbers. *Proc. Edinburgh Math. Soc.*, 54(1):55–65, 2011.

[10] G.L. Cohen and P. Hagis, Jr. On the number of prime factors of n if $\varphi(n)|(n-1)$. *Nieuw Arch. Wisk. (3)*, 28(2):177–185, 1980.

[11] P. Erdös. Some asymptotic formulas in number theory. *J. Indian Math. Soc. (N.S.)*, 12:75–78, 1948.

[12] J.M. Grau and F. Luca. Cullen numbers with the Lehmer property. *Proc. Amer. Math. Soc.*, 140(129–134), 2012.

[13] A.R. Korselt. Problème chinois. *L'intermédiaire des mathématiciens*, 6:142–143.

[14] D. H. Lehmer. On Euler's totient function. *Bull. Amer. Math. Soc.*, 38(10):745–751, 1932.

[15] G. Löh and W. Niebuhr. A new algorithm for constructing large Carmichael numbers. *Math. Comp.*, 65(214):823–836, 1996.

[16] F. Luca. Fibonacci numbers with the Lehmer property. *Bull. Pol. Acad. Sci. Math.*, 55(1):7–15, 2007.

[17] F. Luca and C. Pomerance. On composite integers n for which $\varphi(n) \mid (n-1)$. *Bol. Soc. Mat. Mexicana*, to appear.

[18] R.G.E. Pinch. A note on Lehmer's totient problem. *Poster presented in ANTS VII, http://www.math.tu-berlin.de/∼kant/ants/Poster/Pinch_Poster3.pdf.*

[19] C. Pomerance. On composite n for which $\varphi(n) \mid n-1$. II. *Pacific J. Math.*, 69(1):177–186, 1977.