INFINITUDE OF k-LEHMER NUMBERS WHICH ARE NOT CARMICHAEL

NATHAN MCNEW AND THOMAS WRIGHT

ABSTRACT. In this paper, we prove that there are infinitely many n for which $rad(\varphi(n))|n-1$ but n is not a Carmichael number. Additionally, we prove that for any $k \geq 3$, there exist infinitely many n such that $\varphi(n)|(n-1)^k$ but $\varphi(n) \nmid (n-1)^{k-1}$. The constructs that we consider here are generalizations of Carmichael and Lehmer numbers, respectively, that were first formulated by Grau and Oller-Marcén [GOM].

1. INTRODUCTION

In 1932, D.H. Lehmer [Le] asked the following question:

Lehmer's Question. *Do there exist positive composite integers, n, for which $\varphi(n)|n-1$?*

Here $\varphi(n)$ denotes the Euler totient function of n. Note that any prime number trivially satisfies Lehmer's condition. Composite n satisfying this condition are said to be *Lehmer numbers*, however no such numbers are known. If such a number, n were to exist, it is known that n would have to be greater than 10^{30} and that n would have at least 14 prime factors [CH]. There is currently some disagreement as to whether one should expect Lehmer numbers to exist at all. The best upper bound currently known for their count, due to Luca and Pomerance [LP], is

$$\frac{x^{1/2}}{(\log x)^{1/2+o(1)}}$$

as $x \to \infty$.

In an attempt to better understand the relationship between $\varphi(n)$ and $n-1$, Grau and Oller-Marcén [GOM] suggested the following weakening of the Lehmer condition:

Definition 1.1. *A composite natural number n is called a <u>k-Lehmer number</u> if $\varphi(n)|(n-1)^k$. We denote the set of k-Lehmer numbers by L_k.*

The idea of a Lehmer number can also be weakened in the following manner:

Definition 1.2. *Let $\kappa(n) = rad(\varphi(n))$, where $rad(m)$ denotes the largest squarefree divisor of m. We will call a composite natural number n a <u>radimichael number</u> if*

$$\kappa(n)|n-1.$$

Note that an integer n is a radimichael number if and only if it is a k-Lehmer number for some value of k. The study of Lehmer numbers and their generalizations is closely connected to the study of Carmichael numbers, the pseudoprimes to the Fermat primality test:

Definition 1.3. *A composite number n with the property that $a^n \equiv a \pmod{n}$ for every $a \in \mathbb{Z}$ is called a Carmichael number.*

In 1899 Korselt [Ko] gave the following characterization of Carmichael numbers.

Korselt's Criterion. *A composite natural number n is a Carmichael number if and only if n is squarefree and $p-1|n-1$ for each prime $p|n$.*

Korselt didn't find any examples of Carmichael numbers however. The smallest example, 561, was found by Carmichael [Ca] in 1910, who also gave an equivalent characterization of these numbers which makes their connection with Lehmer numbers more apparent. Define $\lambda(n)$ to be the Carmichael lambda function of n, the smallest integer such that $a^{\lambda(n)} \equiv 1 \pmod{n}$ for every integer a coprime to n. Then n is a Carmichael number if and only if $\lambda(n)|n-1$. (Note that $\varphi(n)$ gives the order of the group $(\mathbb{Z}/n\mathbb{Z})^\times$, while $\lambda(n)$ gives the greatest order of any element of that group.)

Now, since $\kappa(n)|\lambda(n)$, it is clear that any Carmichael number is also a radimichael number (hence the name). However, the converse is not necessarily true; for example, 15 is a radimichael number that isn't Carmichael. In this paper, we study radimichael and k-Lehmer numbers which are not Carmichael.

2. Results

Because the radimichael numbers satisfy a substantially weaker condition than Carmichael numbers, it would be reasonable to expect there to be far more radimichael numbers than Carmichael numbers. This expectation has not been borne out by heuristics or upper bounds, however. The first author [Mc] proved that the best upper bound for the count, $C(x)$, of the Carmichael numbers up to x,

$$C(x) \leq x^{1-(1+o(1))\log\log\log x/\log\log x}$$

as $x \to \infty$, holds for radimichael numbers as well. Furthermore, Pomerance [Po] argues that this bound is heuristically tight. Regardless, it might be reasonable to expect that radimichael numbers would be easier to find than Carmichael numbers.

It has been known since 1994 [AGP] that there are infinitely many Carmichael numbers. From this, it follows trivially that there are also infinitely many radimichael numbers. However, while it has been conjectured by the first author [Mc] that there are infinitely many radimichael numbers which are not Carmichael, this has not previously been demonstrated. In this paper, using the results of Maynard [Ma1] and Tao on primes in tuples, we resolve this conjecture and in particular prove the following:

Theorem 2.1. *There are infinitely many n for which $\kappa(n)|n-1$ but $\lambda(n) \nmid n-1$. Moreover, the number of radimichael numbers up to x is at least $x^{\frac{1}{2}+o(1)}$ as $x \to \infty$.*

For reference's sake, we note that the best lower bound for the count of the Carmichael numbers up to x, due to Harmon [Ha], is $\gg x^{1/3}$. This result then squares with our intuition that radimichael numbers should be easier to find using current mathematical technology.

Using our method of proof we are also able to give a more general result about k-Lehmer numbers. The set of all radimichael numbers, $\bigcup_k L_k$, (where L_k is the set of k-Lehmer numbers) is known to be infinite, since there are infinitely many Carmichael numbers. However, the question of whether there are infinitely many

k-Lehmer numbers for specific values of k has been open. Here, we resolve this question for nearly all values of k:

Theorem 2.2. *For any $k \geq 3$, the set of k-Lehmer numbers which are not $(k-1)$-Lehmer, $L_k \backslash L_{k-1}$, contains infinitely many integers with exactly $k-1$ prime factors. In particular, the count of such numbers up to x is at least $x^{\frac{1}{k-1}+o(1)}$ as $x \to \infty$.*

We remark that as in the previous theorem, the k-Lehmer numbers that we construct are not Carmichael numbers.

In some sense, this result is optimal; as Grau and Oller-Marcén [GOM] proved that there are no 2-Lehmer numbers with exactly two prime factors, we know that it would be impossible to prove a general result about k-Lehmer numbers with exactly k prime factors. This result also highlights the fact that $k = 2$ is a particularly interesting case; unlike 1-Lehmer numbers, it is known that 2-Lehmer numbers exist, but we are still unable to prove that there are infinitely many of them.

We make extensive use of the theorem of Maynard and Tao, combined with a method first introduced in [Wr] to reach our result. The trick is to use k-tuples chosen so that any primes in the tuple can be multiplied to produce a non-Carmichael radimichael number. The second theorem is then simply a matter of counting exactly what sorts of radimichael numbers we have.

3. Invoking the Maynard-Tao Theorem

Recall that Maynard-Tao gives us the following:

Theorem 3.1. *Let $a, b \in \mathbb{N}$ be such that $a \geq 2$, $b \geq 0$. Consider the admissible k-tuple*

$$D_{\{a,b,s\}}(n) = (a^{b+1}n + 1, a^{b+2}n + 1, a^{b+3}n + 1, ..., a^{b+s}n + 1).$$

Then for any m, there exists an integer H_m such that if $s \geq H_m$ then at least m of the s terms above are prime for infinitely many values of n. In particular, the number of values of n up to x for which $D_{\{a,b,s\}}(n)$ contains at least m prime numbers is $\gg_m \frac{x}{\log^s x}$.

The quantitative version stated here is proven in much greater generality in [Ma2].

We begin by showing that this result is sufficient to construct infinitely many radimichael numbers with any fixed number of prime factors; later, we will show that the numbers so constructed are not Carmichael.

Lemma 3.2. *For any choice of $a, m \geq 2$, $b \geq 0$ let $s \geq H_m$, and let n be such that the tuple $D_{\{a,b,s\}}(n)$ contains at least m primes. Label these primes $p_1 < p_2 < ... < p_m$. Then*

$$N = p_1 p_2 ... p_m.$$

is a radimichael number.

Proof. Let $p_1 < p_2 < ... < p_m$ be as above. Write

$$p_i = a^{l_i} n + 1$$

for some $b + 1 \leq l_i \leq b + s$. Then

$$\mathrm{rad}(p_i - 1) = \mathrm{rad}(an)$$

for every i, and so

$$\kappa(N) = \mathrm{rad}((p_1 - 1)(p_2 - 1)\cdots(p_m - 1)) = \mathrm{rad}(an)$$

By construction, we have that

$$p_i \equiv 1 \pmod{an},$$

which means that

$$N \equiv 1 \pmod{an},$$

and so $\kappa(N)|N - 1$. □

Because any Carmichael number must have at least 3 prime factors, this is already sufficient to prove Theorem 2.1:

Proof of Theorem 2.1. Apply Lemma 3.2 in the case $a = 2$, $b = 0$, $m = 2$. For sufficiently large x, Theorem 3.1 implies that the count of the number of n less than $\frac{x^{1/2}}{a^{H_2+1}}$ where at least two of the elements of $D_{\{2,0,H_2\}}(n)$ are prime is $\gg \frac{\sqrt{x}}{\log^{H_2} x}$.

For each such n, we use Lemma 3.2 to produce a radimichael number which is the product of two distinct primes, each less than or equal to $a^{H_2}n+1 \leq \sqrt{x}$. Thus as $x \to \infty$ we obtain $x^{1/2+o(1)}$ radimichael numbers of size at most x. Furthermore, none of these numbers are Carmichael as each has only two prime factors. □

We note here that the idea of using a version of the k-tuple conjecture to prove statements about pseudoprimes is not new; Chernick [Ch] used a stronger (conjectural) version of the Maynard-Tao theorem to prove conditionally that there are infinitely many Carmichael numbers with exactly m prime factors for any $m \geq 3$. However, Chernick's theorem has never been made unconditional (for any value of m), which means that our theorem in the radimichael case is stronger than what can be proven for Carmichael numbers.

4. Radimichael but not Carmichael

In this section, we prove that none of the radimichael numbers constructed using the method of Lemma 3.2 can be Carmichael numbers. Since we can use our method to construct a radimichael number with m prime factors for any value of $m \geq 2$, this then proves that there are infinitely many non-Carmichael radimichael numbers with any fixed number (at least two) of prime factors.

Lemma 4.1. *Let $N = p_1p_2....p_m$ be a radimichael number found by the method of Lemma 3.2. Then N is not a Carmichael number.*

Proof. Let N be such a radimichael number, constructed from a tuple $D_{\{a,b,s\}}(n)$ containing m prime factors. As before, we will write

$$p_i = a^{l_i}n + 1$$

with $l_1 < l_2 < \ldots < l_m$. By Korselt's Criterion, we know that if N is a Carmichael number then

$$a^{l_i}n|N - 1$$

for each i. Specifically that this implies that

$$N \equiv 1 \pmod{a^{l_2}n}.$$

Now, for each $i \geq 2$, $p_i \equiv 1 \pmod{a^{l_2}n}$. So

$$N \equiv p_1 \equiv 1 \pmod{a^{l_2}n}.$$

But this is impossible, since $a^{l_2}n > p_1$ and $N > 1$. □

Remark: We note that this proof is similar in structure to a proof that appears in [Wr], wherein the author uses this method to prove that there cannot exist a Carmichael number N such that the prime factors of N are all Fermat primes.

5. k-Lehmer with $k-1$ factors

Let us now turn our attention to categorizing these radimichael numbers by their k-Lehmer properties. We are now able to give a proof of Theorem 2.2. In particular we show that for each $k \geq 3$ there exist infinitely many k-Lehmer numbers (which are neither $(k-1)$-Lehmer numbers nor Carmichael numbers) with $k-1$ prime factors and that the count of such integers up to x is at least $x^{\frac{1}{k-1}+o(1)}$ as $x \to \infty$.

Proof of Theorem 2.2. Let $m = k-1$ and fix an integer $a \geq 2$. For $b = mH_m$, consider the tuple

$$D_{\{a,b,H_m\}}(n) = (a^b n + 1, a^{b+1}n + 1, a^{b+2}n + 1, ..., a^{b+H_m}n + 1).$$

Theorem 3.1 implies that there are infinitely many n for which at least m of these forms are simultaneously prime infinitely often, and using Lemma 3.2 we see that the product of these m primes is a radimichael number. Moreover, as in the proof of Theorem 2.1, we find that there are $\gg_m x^{1/m+o(1)}$ values of n where all of the resulting m primes have size at most $cx^{1/m}$, where c is chosen in such a way that the product of the primes has size at most x. We will now see that the resulting radimichael numbers are in fact k-Lehmer numbers.

For a set of primes $p_1,\ldots,p_m$ coming from this tuple, write $p_i = a^{b+l_i}n+1$ where $l_i < l_j$ if $i < j$. Let $N = p_1 \cdots p_m$. Then

$$\varphi(N) = \varphi(p_1)\cdots\varphi(p_m) = a^{l_1+\cdots+l_m+mb}n^m.$$

Note that $l_1 \geq 1$ and $l_m \leq H_m$. Additionally, $N-1$ can be expanded out as

$$N - 1 = a^{mb+l_1+l_2+\cdots+l_m}n^m + \cdots + \left(\sum_{i=1}^{m} a^{b+l_i}\right) n. \tag{1}$$

We show first that $\varphi(N)|(N-1)^{m+1}$. It is clear that $a^{b+l_1}n$ divides every term of the expression above. So

$$a^{b+l_1}n|N-1,$$

and hence

$$(a^{b+l_1}n)^j|(N-1)^j.$$

Now, if we let $j = m+1$ then

$$a^{l_1+\cdots+l_m+mb}n^m|(a^{b+l_1}n)^{m+1},$$

since $\sum_i l_i < mH_m = b$. So $\varphi(N)|(N-1)^{m+1}$ and thus N is a k-Lehmer number.

On the other hand, raising equation (1) to the m and expanding, we can write

$$(N-1)^m = a^{mb+ml_1}n^m + Y$$

where $a^{mb+ml_1+1}n^m|Y$. Thus $(N-1)^m$ is not divisible by $a^{mb+ml_1+1}n^m$ while $\varphi(N)$ is, so N cannot be a $(k-1)$-Lehmer number.

□

Finally, we note that in contrast to the construction here showing that there are at least $x^{\frac{1}{k-1}+o(1)}$ k-Lehmer numbers with $k-1$ prime factors, it was shown in [Mc] that the number of k-lehmer numbers up to x is $\ll_k x^{1-\frac{1}{4k-1}}$, and that the number of radimichael numbers with m prime factors is $\ll x^{1-\frac{1}{2m}}$. In the special case that $m=2$ the count of radimichael numbers with 2 prime factors is less than

$$x^{1/2}\exp\left\{\frac{2(2\log x)^{1/2}}{\log\log x}\left(1+O\left(\frac{1}{\log\log x}\right)\right)\right\}=x^{1/2+o(1)}$$

as $x\to\infty$. So, our lower bound for the count of radimichael numbers with two prime factors is nearly optimal.

References

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

[Ca] R. D. Carmichael, *Note on a new number theory function*, Bulletin of the American Mathematical Society, **16** (1910), 232-238.

[Ch] J. Chernick, *On Fermats simple theorem*, Bull. Amer. Math. Soc. **45** (1939), 269-274.

[CH] 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** (1980), no. 2, 177-185.

[GOM] J. M. Grau and A. M. Oller-Marcén, *On k-Lehmer numbers*, Integers **12** A37 (2012), 1081-1089.

[Ha] G. Harmon *Watt's mean value theorem and Carmichael numbers.* Int. J. Number Theory **4** (2008), 241-248.

[Ko] A. Korselt, Problème chinois, L'intermediaire des math., **6** (1899) 142-143.

[Le] D. H. Lehmer, *On Euler's totient function*, Bull. Amer. Math. Soc. **38** (1932), no. 10, 745-751.

[LP] F. Luca and C. Pomerance, *On composite integers n for which* $\varphi(n)|n-1$, Boletin de la Sociedad Matemtica Mexicana, **17** (2011), 13-21.

[Ma1] J. Maynard, *Small gaps between primes*, Ann. of Math. (2) **181** (2015), 383-413.

[Ma2] J. Maynard, *Dense clusters of primes in subsets*, preprint, arXiv:1405.2593.

[Mc] N. McNew, *Radically weakening the Lehmer and Carmichael conditions*, Int. J. Number Theory **9** (2013), 1215-1224.

[Po] C. Pomerance, *Two methods in elementary analytic number theory*, Number theory and applications (Banff, AB, 1988), NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., vol. 265, Kluwer Acad. Publ., Dordrecht, 1989, pp. 135-161.

[Wr] T. Wright, *The impossibility of certain types of Carmichael numbers*, Integers, **12** A31 (2012), 1-13.

Department of Mathematics, Towson University, 7800 York Road, Towson, MD 21204
E-mail address: nmcnew@towson.edu

Department of Mathematics, Wofford College, 429 N. Church St., Spartanburg, SC 29302
E-mail address: wrighttj@wofford.edu