J. Aust. Math. Soc. **100** (2016), 421–429
doi:10.1017/S1446788715000427

FACTORS OF CARMICHAEL NUMBERS AND A WEAK *k*-TUPLES CONJECTURE

THOMAS WRIGHT

(Received 11 February 2015; accepted 23 March 2015; first published online 17 November 2015)

Communicated by I. E. Shparlinski

Abstract

In light of the recent work by Maynard and Tao on the Dickson k-tuples conjecture, we show that with a small improvement in the known bounds for this conjecture, we would be able to prove that for some fixed R, there are infinitely many Carmichael numbers with exactly R factors for some fixed R. In fact, we show that there are infinitely many such R.

2010 *Mathematics subject classification*: primary 11A51.

Keywords and phrases: Carmichael numbers, Dickson's conjecture, prime k-tuples, pseudoprimes.

1. Introduction

Recall that a Carmichael number [Ca] is a composite number n for which

$$a^n \equiv a \bmod n$$

for every $a \in \mathbb{Z}$.

Although Carmichael numbers were proven to be infinite in number in 1994 in a paper by Alford *et al.* [AGP], there are still many open conjectures about Carmichael numbers that we cannot begin to address. Chief among those conjectures is the following theorem.

CONJECTURE. For any $R \in \mathbb{N}$ with $R \geq 3$, there exist infinitely many Carmichael numbers with R prime factors.

In fact, specific conjectures [GP] have been made about the number of Carmichael numbers up to x with specific numbers of prime factors.

GRANVILLE–POMERANCE CONJECTURE. For any $R \in \mathbb{N}$ with $R \geq 3$, let $C_R(x)$ denote the number of Carmichael numbers up to x with exactly R factors. Then

$$C_R(x) = x^{(1/R)+o_R(1)}.$$

Up to this point, most of the work done on this conjecture has focused on upper bounds. The only affirmative results that we have been able to prove about lower bounds for the number of factors of a given Carmichael number are that (a) there exist Carmichael numbers with arbitrarily large numbers of factors, (b) for any a and M, there are infinitely many Carmichael numbers where the number of prime factors is congruent to $a \mod M$, and (c) for any k with $3 \leq k \leq 19\,565\,220$, there exists at least one Carmichael number with k prime factors [AGHS]. Most other statements about Carmichael numbers with fixed numbers of prime factors have been considered to be beyond current methods.

In this paper, we show that recent progress on the Dickson k-tuples conjecture has *almost* got us to the point where we can prove a lower bound for least one (and, in fact, for infinitely many) values of R. In the next section, we introduce the Dickson conjecture and show how it can be used in the study of Carmichael numbers.

1.1. The *k*-tuples conjecture. Before we state Dickson's conjecture, we must first note an important criterion for determining whether a number is Carmichael. In 1899, Korselt [Ko] posed the following necessary and sufficient condition for determining whether a number is a Carmichael number.

KORSELT'S CRITERION. A natural number n is a Carmichael number if and only if n is square-free and composite and for every prime p that divides n, $p - 1 | n - 1$.

Now let us define the Dickson k-tuples conjecture. For a set $D = \{a_1z + b_1, a_2z + b_2, \ldots, a_kz + b_k\}$ of distinct linear forms with all $a_i > 0$, we will call the set *admissible* if it contains no local obstructions, that is, for any p, there exists a $z \in \mathbb{N}$ such that

$$p \nmid \prod_{i=1}^{k} (a_iz + b_i).$$

Dickson's conjecture can now be stated as follows.

DICKSON'S k-TUPLE CONJECTURE. Let $D = \{a_1z + b_1, a_2z + b_2, \ldots, a_kz + b_k\}$ be an admissible set of k linear forms. If $k \geq 2$, then there exist infinitely many z for which all of the forms in D are simultaneously prime.

Note that in the case of $k = 1$, the above is not a conjecture but rather Dirichlet's theorem.

Many years ago, mathematicians began to realize that the search for Carmichael numbers would be made easier if Dickson's conjecture were true. The first to come to this realization was Chernick [Ch], who in 1939 noted that if all three of $6z + 1$, $12z + 1$, $18z + 1$ are simultaneously prime, then

$$(6z + 1)(12z + 1)(18z + 1)$$

https://doi.org/10.1017/S1446788715000427 Published online by Cambridge University Press

is a Carmichael number by Korselt's criterion. Chernick listed a number of other tuples that could be converted into Carmichael numbers as well, including

$$(12z+5)(36z+13)(48z+17),$$
$$(30z+7)(60z+13)(150z+31),$$
$$(180z+7)(300z+11)(360z+13)(1200z+41),$$

and so on. It is an easy exercise to prove that the assumption of Chernick's conjecture would prove the Granville–Pomerance conjecture with the correct lower bounds.

Of course, using Chernick's methods to prove that there are infinitely many Carmichael numbers would require the full version of Dickson's conjecture for some tuple, which still seems to be a good distance from fruition. Recently, though, weaker versions of Dickson's conjecture have actually become available to us; in 2013, Maynard and Tao [May] proved the following result.

Maynard–Tao theorem. *Let $D = \{z+b_1, z+b_2, \ldots, z+b_k\}$ be a set of k admissible linear forms. For any $m \geq 2$, there exists a constant C such that if $k > Ce^{8m}$ then m of the forms in D are prime infinitely often.*

Recent improvements by the Polymath project have reduced this bound to approximately Ce^{4m} (as of this writing).

Unfortunately, a relationship between m and k with k roughly equal to e^{4m} does not *quite* appear to be strong enough to help us in the search for Carmichael numbers. In this paper, we determine how much further these results need to go.

1.2. Main theorem. For the results of this paper to hold, we would need the following strengthening of the Maynard–Tao theorem (or weakening of Dickson's conjecture).

Weak Version of k-tuple conjecture. As before, let $D = \{a_1z+b_1, a_2z+b_2, \ldots, a_kz+b_k\}$ be a set of k admissible linear forms. There exists a fixed constant $T \geq 1$ such that for any $m \geq 2$, if $k \geq m^T$, then m of the forms in D are prime infinitely often.

The full conjecture, of course, would be for $T = 1$.

We note here that the exact value of T is irrelevant; for this result to hold, we only require that the relationship between m and k be polynomial and not exponential[1]. If this statement were known to be true, we would immediately have the following result.

Main theorem. *Assume that the k-tuples conjecture above is true. Let $C_R(x)$ denote the number of Carmichael numbers up to x with exactly R prime factors. Then there exists an R for which $C_R(x) \to \infty$ as $x \to \infty$. In fact, there are infinitely many R for which $C_R(x) \to \infty$ as $x \to \infty$.*

[1] Our methods can actually be extended slightly—but only slightly—beyond polynomial. If the conjecture replaced k^T with $e^{(\log k)^{\theta-\epsilon}}$ for some $\epsilon < \theta$ (and $\epsilon > 0$) with θ as defined in Lemma 3.1, the methods below would still work.

https://doi.org/10.1017/S1446788715000427 Published online by Cambridge University Press

If we are given a specific T, we can actually calculate an upper bound for the smallest R for which $C_R(x) \to \infty$ as $x \to \infty$. Here, we show that if T is large then this upper bound can be given by

$$2^{T^{3/(\theta-1)}/\log(T^{3/(\theta-1)})}, \tag{1.1}$$

where θ is the constant defined in Lemma 3.1.

2. Sketch of proof

Traditionally, a proof of infinitely many Carmichael numbers follows the following rubric, which was originally posed in [AGP]. First, we prove that there are many integers L for which $\lambda(L)$, the maximum order of an element mod L, is small relative to L. For each L, we prove that there exists some z for which there are many primes of the form $dz + 1$ with $d|L$. Having found sufficiently many of these primes, we prove that some subsets of these primes multiply to 1 mod zL; hence, each of these subsets is such that the product of all primes in a given subset yields a Carmichael number. Since we can prove that there are infinitely many choices of L (and since we can prove that choosing a larger L will generate new Carmichael numbers), there are infinitely many Carmichael numbers.

While this method can be successfully used to prove that there are infinitely many Carmichael numbers, it lacks the ability to prove anything about Carmichael numbers with a fixed number of factors. The reason is that we have no control over the size of L and, as L grows larger, the number of primes $dz + 1$ required to guarantee a product of 1 mod zL grows larger as well. This ever-growing L is the reason that we have been able to prove the existence of Carmichael numbers with arbitrarily large numbers of factors; however, it is of no help for fixed numbers of factors.

The conjecture stated above, however, allows for a significant simplification of the argument in [AGP]. In particular, for a given L, we can now prove that there are an infinitude of z such that $dz + 1$ is prime for many values of $d|L$; for each of these z, we can then prove that there exist Carmichael numbers where all prime factors are of this form $dz + 1$. As such, we can show that there are infinitely many Carmichael numbers for a single choice of L. Since each choice of L and z will have a limited number of possible factors, we can see that there will be some fixed number R that has many Carmichael numbers with R prime factors. By strategically changing our L, we can change R as well and thus we see that there are infinitely many such R.

Unfortunately, we are still well short of being able to pin down an exact value for R. This is a result of the fact that the weakened k-tuples conjecture above is similarly ambiguous; if the full strength of the k-tuples conjecture were realized, one could prove our theorem for every fixed $R \geq 3$.

It is interesting to note that, using the original methods of [AGP], one can very quickly prove that there are infinitely many Carmichael numbers n for which the number of prime factors of n is at most $e^{(\log\log n)^{1/\theta}}$ (where θ is as in Lemma 3.1). It may be possible that the new Maynard–Tao results would yield an improvement in this bound. We plan to take this issue up in a future paper.

https://doi.org/10.1017/S1446788715000427 Published online by Cambridge University Press

3. Finding an L

First, we must find an L for which it is suitable to set up our k-tuple. For this, we recall the following result.

Let $1 < \theta < 2$ and let $P(q-1)$ be the size of the largest prime divisor of $q-1$. Define the set Q to be

$$Q = \left\{ q \text{ prime} : \frac{y^\theta}{\log y} \le q \le y^\theta, P(q-1) \le y \right\}.$$

Throughout this paper, we will assume that y is greater than some constant Y, where Y is chosen such that bounds on the density of smooth primes can be invoked and that y^θ grows sufficiently large relative to constants. This constant could undoubtedly be made effective with some work; we do not do so here.

With this caveat, the following result can be easily shown.

Lemma 3.1. *For Q as above, there exists a constant γ_θ such that*

$$|Q| \ge \gamma_\theta \frac{y^\theta}{\log(y^\theta)}.$$

Proof. The proof is merely an application of Bombieri–Vinogradov; it appears in [AGP, Ma, Wr] and others.

For $v < z$, let us denote by $\pi(z, v)$ the number of primes q less than z such that $P(q-1) \le v$. Let $\frac{1}{2} < \alpha < \frac{2}{3}$ and define $\epsilon = \epsilon(\alpha) < \alpha - \frac{1}{2}$. Note that if $q \le z$ is such that q can be written as $q = 1 + q'k$ for some prime $q' \in [z^{1-\alpha}, z^{(1/2)-\epsilon}]$, then $P(q-1) \le z^\alpha$; each q has at most two such representations. So,

$$\pi(z, z^\alpha) \ge \frac{1}{2} \sum_{q' \in \mathbb{P}, z^{1-\alpha} \le q' \le z^{(1/2)-\epsilon}} \# \left\{ q \text{ prime}, \frac{z}{\log z} \le q \le z, q \equiv 1 \bmod q' \right\}.$$

Since q is sufficiently large relative to q', we may use Bombieri–Vinogradov to find that

$$\pi(z, z^\alpha) \ge \sum_{q' \in \mathbb{P}, z^{1-\alpha} \le q' \le z^{(1/2)-\epsilon}} \frac{z}{\phi(q') \log z} \ge \log\left(\frac{\frac{1}{2} - \epsilon}{1 - \alpha} \right) \frac{z}{\log z}.$$

The lemma then follows by letting $z = y^\theta$, $\alpha = \min\{(1/\theta), \frac{3}{5}\}$, and $\gamma = \log((1/2 - \epsilon)/(1 - \alpha))$. □

We note that this is not the best possible bound; however, we do not require best possible here, and this proof is relatively straightforward.

From this, we let

$$L = \prod_{q \in Q} q.$$

https://doi.org/10.1017/S1446788715000427 Published online by Cambridge University Press

4. The size of $\lambda(L)$

In this section, we determine the size of $\lambda(L)$ and how large we would like our tuple to be.

To begin, we state a theorem that appears in the paper of Alford *et al.* [AGP, Proposition 1.2]. For an abelian group G, $n(G)$ will denote the smallest number such that a collection of at least $n(G)$ elements must contain some subset whose product is the identity. From van Emde Boas and Kruyswijk [EK] and Meshulam [Me],

$$n(G) \leq \lambda(G)\left(1 + \frac{\log|G|}{\lambda(G)}\right).$$

With this notation, we now state the theorem.

THEOREM 4.1. *Let G be a finite abelian group and let $s > t > n = n(G)$ be integers. Then any sequence of s elements of G contains at least $\binom{r}{t}/\binom{r}{n}$ distinct subsequences of length at most t and at least $t - n$ whose product is the identity.*

This theorem is proven elsewhere, so we do not give the proof here; the interested reader can consult the references given above.

In order to invoke our theorem, we must now compute the size of $\lambda(L)$. To this end, we have the following result.

LEMMA 4.2. *We have $\lambda(L) \leq e^{2\theta y}$.*

PROOF. We recall that, by construction, any prime factor of L is at most y. Since any prime factor of $\lambda(L)$ must divide $q - 1$ for some $q|L$, we see that any prime factor of $\lambda(L)$ must be less than y as well. Let a_q be the largest power of q such that $q^{a_q} \leq y^{\theta}$. It follows, then, that

$$\lambda(L) \leq \prod_{q \leq y} q^{a_q} \leq y^{\theta\pi(y)} \leq e^{2\theta y}. \qquad \square$$

By abuse of notation, we will use $n(L)$ to denote $n(G)$ for the group $(\mathbb{Z}/L\mathbb{Z})^{\times}$. We may now combine Lemma 4.2 and Theorem 4.1 to find the following result.

LEMMA 4.3. *We have*

$$2n(L) \leq e^{3\theta y}.$$

5. Our k-tuple and the size of $\lambda(L)$

Finally, we define our admissible set and prove that it is sufficiently large to generate a Carmichael number. Let our set D be as follows:

$$D = \{dz + 1 : 1 \leq d \leq L, d|L\}.$$

For those who have seen [AGP], this is a familiar construction; however, in the present case we are not forced to make any requirement that the $dz + 1$ be prime (as the conjecture will take care of that for us).

The size of D is of course determined by the number of factors of L.

Lemma 5.1. *For the set D defined as above,*

$$|D| \geq 2^{\gamma(y^{\theta}/\log y^{\theta})}.$$

Let us assume the conjecture for some value of T. We will choose a y (and hence an L) large enough to trigger the conjecture. Letting

$$W = \max\left\{T, \frac{10\theta}{\gamma(\theta-1)\ln 2}\right\},$$

we define

$$y = \max\{W^{3/(\theta-1)}, Y\}.$$

Theorem 5.2. *Assuming the weak version of the k-tuples conjecture as stated in the introduction, there exists a set D of linear forms that has more than $2n(L)$ primes infinitely often. In other words, there are infinitely many Carmichael numbers with a fixed number R of prime factors, where*

$$R \leq |D| \leq \max\{2^{W^{3/(\theta-1)}/\log(W^{3/(\theta-1)})}, 2^{Y^{\theta}/\log Y^{\theta}}\}.$$

Clearly, if T is large, the first of the terms in the max will be the relevant one; this is the bound given in (1.1).

Proof. We prove this theorem by comparing $|D|$ to $2n(L)$. To do this, we examine the ratio of the logarithms of the two terms. First, if $W^{3/(\theta-1)} > Y$, then

$$\begin{aligned}\frac{\log|D|}{\log(2n(L))^{T}} &\geq \frac{(\ln 2)\gamma\frac{W^{3\theta/(\theta-1)}}{(\frac{3}{\theta-1})\log W}}{3\theta(W^{3/(\theta-1)})W}\\ &\geq \frac{(\ln 2)\gamma(\theta-1)}{9\theta}\frac{W^{2}}{\log W}\\ &> \frac{(\ln 2)\gamma(\theta-1)}{9\theta}W\\ &> 1.\end{aligned}$$

If $W^{3/(\theta-1)} > Y$, then $T < Y^{(\theta-1)/3}$ and hence

$$\begin{aligned}\frac{\log|D|}{\log(2n(L))^{T}} &\geq \frac{(\ln 2)\gamma\frac{Y^{\theta}}{\theta\log Y}}{3\theta YT}\\ &\geq \left(\frac{\gamma\ln 2}{3\theta^{2}\log Y}\right)Y^{(2/3)(\theta-1)}\\ &> 1.\end{aligned}$$

In both cases, $|D| > (2n(L))^{T}$. So, if $|D| = M$, then there exist infinitely many z for which D has at least $2n(L)$ primes simultaneously.

Let $z \in \mathbb{N}$ be such that D has at least $2n(L)$ primes. By [AGP, Theorem 1], this means that some subset of those primes will multiply to 1 mod L.

https://doi.org/10.1017/S1446788715000427 Published online by Cambridge University Press

Let $p_1, p_2, \ldots, p_r$ be such a subset. Since each p_i is also congruent to 1 mod z,

$$m = p_1 p_2 \ldots p_r \equiv 1 \bmod Lz.$$

This means that for each p_i, we have $p_i - 1 | Lz | m - 1$. Thus, by Korselt's criterion, m is a Carmichael number. Since there are infinitely many such z, there are infinitely many Carmichael numbers where the number of factors is $\leq |D|$; thus, there must exist an $R \leq |D|$ such that infinitely many Carmichael numbers have exactly R factors.

For the upper bound on D, we note simply that

$$|D| \leq 2^{y^\theta / \log y^\theta}.$$

The bound in the theorem is then found by replacing y with its definition. □

From here, it is small step to the proof that there are infinitely many such R.

Theorem 5.3. *Assuming our weak version of Dickson's conjecture,* $C_R(x) \to \infty$ *as* $x \to \infty$ *for infinitely many choices of* R.

Proof. Assume not. Then there is some bound J such that if there are infinitely many Carmichael numbers with R prime factors, then $R < J$.

Choose a y (and, consequently, an L) such that

$$\log |D| > 2TJ.$$

From our conjecture, we know that there exist infinitely many z for which the number of primes in D is $> 2J$. Also, from the work above, we know that the number of primes in D is $> 2n(L)$. Thus, if we choose $t \geq \max\{2J, 2n(L)\}$, Theorem 4.1 says that a Carmichael number generated by our method will have at least $t - n(L)$ factors. Since $t - n(L) > n(L)$ and $t - n(L) \geq (t/2) \geq J$, there are infinitely many such Carmichael numbers with at least J and at most $|D|$ factors, contradicting our assumption. □

Acknowledgement

The author would like to thank the referee for helpful comments and suggestions.

References

[AGHS] W. R. Alford, J. Grantham, S. Hayman and A. Shallue, 'Constructing Carmichael numbers through improved subset-product algorithms', *Math. Comp.* **83** (2014), 899–915.

[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', *Bull. Amer. Math. Soc.* **16** (1910), 232–238.

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

[EK] P. Van Emde Boas and D. Kruyswijk, 'A combinatorial problem on finite Abelian groups III', Report ZW 1969-008, Stichting Mathematisch Centrum, Amsterdam, 1969.

[GP] A. Granville and C. Pomerance, 'Two contradictory conjectures concerning Carmichael numbers', *Math. Comp.* **71** (2002), 883–908.

[Ko] A. Korselt, 'Problème chinois', *L'intermédinaire des Mathématiciens* **6** (1899), 142–143.

https://doi.org/10.1017/S1446788715000427 Published online by Cambridge University Press

[Ma] K. Matomäki, 'On Carmichael numbers in arithmetic progressions', *J. Aust. Math. Soc.* **2** (2013), 1–8.

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

[Me] R. Meshulam, 'An uncertainty inequality and zero subsums', *Discrete Math.* **84**(2) (1990), 197–200.

[Wr] T. Wright, 'Infinitely many Carmichael numbers in arithmetic progressions', *Bull. Lond. Math. Soc.* **45** (2013), 943–952.

THOMAS WRIGHT, Department of Mathematics, Wofford College,
429 N. Church St., Spartanburg, SC 29302, USA
e-mail: wrighttj@wofford.edu

https://doi.org/10.1017/S1446788715000427 Published online by Cambridge University Press