Bull. Aust. Math. Soc. **99** (2019), 376–384
doi:10.1017/S0004972719000133

FACTORS OF CARMICHAEL NUMBERS AND AN EVEN WEAKER *k*-TUPLES CONJECTURE

THOMAS WRIGHT

(Received 8 June 2018; accepted 25 August 2018; first published online 20 February 2019)

Abstract

One of the open questions in the study of Carmichael numbers is whether, for a given $R \geq 3$, there exist infinitely many Carmichael numbers with exactly R prime factors. Chernick ['On Fermat's simple theorem', *Bull. Amer. Math. Soc.* **45** (1935), 269–274] proved that Dickson's k-tuple conjecture would imply a positive result for all such R. Wright ['Factors of Carmichael numbers and a weak k-tuples conjecture', *J. Aust. Math. Soc.* **100**(3) (2016), 421–429] showed that a weakened version of Dickson's conjecture would imply that there are an infinitude of R for which there are infinitely many such Carmichael numbers. In this paper, we improve on our 2016 result by weakening the required conjecture even further.

2010 *Mathematics subject classification*: primary 11A51; secondary 11A41.

Keywords and phrases: Carmichael number, Granville–Pomerance conjecture, Dickson's k-tuple conjecture.

1. Introduction

Let us begin with a definition.

Definition 1.1. A *Carmichael number* is a composite number n for which

$$a^n \equiv a \pmod{n}$$

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

Of course, Fermat's little theorem states that $a^p \equiv a \pmod{p}$ is always true if p is prime. Carmichael numbers, then, are the counterexamples which disprove the converse of Fermat's little theorem.

Although it was proved that there are infinitely many Carmichael numbers in 1994 [1], a number of open questions about Carmichael numbers still remain. One such problem is the following question.

Question 1.2. Let R be an integer such that $R \geq 3$. Are there infinitely many Carmichael numbers with exactly R prime factors?

It is believed that there are infinitely many Carmichael numbers with exactly R prime factors for any $R \geq 3$. In fact, specific conjectures [7] have been made about the number of Carmichael numbers up to x with a given number of prime factors.

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

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

At present, we are unable to prove even that there exists an R such that there exist infinitely many Carmichael numbers with exactly R prime factors. Alford, Granville, and Pomerance's proof [1] that there are infinitely many Carmichael numbers was accomplished by constructing Carmichael numbers with ever-increasing numbers of prime factors; as such, their methods cannot be easily modified to deal with the case where the number of prime factors is limited.

2. Current results

The closest we have come to a substantial result toward the Granville–Pomerance conjecture above was in [13], wherein the present author was able to prove that such an R exists under the assumption of a strong conjecture. To explain the conjecture, we first recall Dickson's conjecture.

CONJECTURE 1 (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; in other words, let D be a set of forms such that for any prime p, there exists a z such that none of the forms are congruent to 0 modulo p. If $k \geq 2$ then there exist infinitely many z for which all of the forms in D are simultaneously prime.

In 1935, Chernick [3] introduced this conjecture to the study of Carmichael numbers when he proved the following result.

THEOREM 2.1 (Chernick, 1935). *Assume Dickson's k-tuple Conjecture (Conjecture 1). Then there are infinitely many Carmichael numbers with exactly 3 prime factors.*

Chernick also showed how one would find infinitely many Carmichael numbers with four and five prime factors; these cases also required the full use of Dickson's conjecture.

The next progress came in 2015, when the present author [13], was able to make use of the following weakened form of Dickson's conjecture.

CONJECTURE 2 (Dickson's k-tuple conjecture (weak version)). As before, let $D = \{a_1z + b_1, a_2z + b_2, \ldots, a_kz + b_k\}$ be an admissible set of k linear forms. There exists a fixed constant $T > 1$ such that for any $m \geq 2$, if $k \geq m^T$ then m of the forms in D are prime infinitely often.

Armed with this conjecture, we were then able to prove the following result.

https://doi.org/10.1017/S0004972719000133 Published online by Cambridge University Press

Theorem 2.2 (Wright, 2016). *Assume the weak version of Dickson's k-tuple conjecture (Conjecture 2). Let $C_R(x)$ denote the number of Carmichael numbers up to x with exactly R prime factors. Then there are infinitely many R for which $C_R(x)$ goes to infinity as x goes to infinity.*

Recent work of Maynard and Tao [9] has given us the following progress toward Dickson's conjecture.

Theorem 2.3 (Maynard–Tao theorem). *Let $D = \{a_1z + b_1, a_2z + b_2, \dots, a_kz + b_k\}$ be a set of k admissible linear forms. For any $m \geq 2$, if $k \geq e^{3.91m}$ then m of the forms in D are prime infinitely often.*

The weak version of Dickson's k-tuple conjecture is still quite a distance from the Maynard–Tao result; it requires a polynomial relationship, while Maynard–Tao only gives an exponential one.

3. New results

This paper attempts to bridge the gap between what was proved in [13] and what is known via Maynard–Tao [9]. We are able to improve the 2016 result to the point where it is *almost* unconditional. To do so, let us introduce the following even weaker version of Dickson's conjecture.

Conjecture 3 (Dickson's *k*-tuple conjecture (even weaker version)). Again, let

$$D = \{a_1z + b_1, a_2z + b_2, \dots, a_kz + b_k\}$$

be a set of k admissible linear forms. There exists a fixed constant $T \geq 1$ such that for any sufficiently large m, if $k \geq e^{m^{1/(\log\log m)^T}}$ then m of the forms in D are prime infinitely often.

Our main result is the following theorem.

Theorem 3.1 (Main Theorem). *Assume the even weaker version of Dickson's k-tuple conjecture (Conjecture 3). Let $C_R(x)$ denote the number of Carmichael numbers up to x with exactly R prime factors. Then there are infinitely many R for which $C_R(x)$ goes to infinity as x goes to infinity.*

4. Methods

The traditional proof of infinitely many Carmichael numbers as laid out in [1] requires us to find many primes q for which $P(q-1)$ (the largest prime divisor of $q-1$) is small. (In [1], 'small' is defined to be less than $q^{1/2}$.) This allows us to construct a number L, defined to be the product of these q's, where the maximum order $\lambda(L)$ of an element (mod L) is fairly small relative to L. We then construct primes p of the form $dk + 1$, where $d|L$ and k is a constant that is common to all of the $p - 1$.

In our proof, however, we will need $\lambda(L)$ to be even smaller—specifically logarithmic—relative to L. Ideally, we could accomplish this by taking primes q for

https://doi.org/10.1017/S0004972719000133 Published online by Cambridge University Press

which $P(q-1)$ is on the order of $\log q$, but unfortunately, no known theorem would allow anything close to this.

The remedy we introduce in this proof is to be somewhat more intentional in our construction of these q. In particular, we construct our smaller primes q in the same way that we construct the larger primes p. Let us take a J made up of many prime factors. We will take our q to be of the form $gl+1$, where $g|J$ (and hence $P(g)$ is of size $\log q$) and l is some parameter that is common to all of the q. This is the goal of Section 5.

Once we have our small primes q, we multiply them together to find L. In Section 6, we show that $\lambda(L)$ is, in fact, very small relative to L. Having constructed L, we simply apply Dickson's conjecture (as stated above) to the tuple

$$D = \{2dk+1 : d|L\}.$$

Sections 7 and 8 show that this tuple is large enough so that some subset of the primes found from it will yield a Carmichael number.

5. The product of small primes

Let us now begin the proof of the Main Theorem. In the first section of the proof, we will construct our q's with this new method of construction.

To start, let z be some large positive number. Let us then define J' by

$$J' = \prod_{r \text{ prime},\ z^{1/2}<r<z} r.$$

As is standard, let $\pi(x,d,a)$ denote the number of primes up to x that are congruent to a (mod d). Fix B such that $0<B<5/12$. Theorem 2.1 of [1] says that for any x there exists a set of integers $\mathcal{S}_B(x)$, where $|\mathcal{S}_B(x)|$ is bounded by some constant S_B, such that if d is not divisible by an element in $\mathcal{S}_B(x)$ and $d \le x^B$ then

$$\pi(x,d,a) \ge \frac{\pi(x)}{2\phi(d)},$$

for any a with $(a,d)=1$. To use this estimate, we must be careful that our moduli are not divisible by an element of $\mathcal{S}_B(x)$. As such, for each element $c \in \mathcal{S}_B(x)$, pick a prime s_c that divides c, and define

$$S = \{s_c : c \in \mathcal{S}_B(x)\}.$$

We can then define

$$J = \prod_{r|J',r\notin S} r.$$

Now, let us define

$$Q_l = \{q \text{ prime} : q = gl+1, g|J\}.$$

In [1], it is shown that there must exist an l with many such primes. We perform a similar proof here.

https://doi.org/10.1017/S0004972719000133 Published online by Cambridge University Press

THEOREM 5.1. *Let $B < 5/12$, and let J be as above. Then there exists an $l \le x^{1-B/2}$ with $(k, L) = 1$ such that*

$$|Q_l| \ge 2^{z/(2\log z)}.$$

PROOF. A similar (though not identical) proof appears in [1, Theorem 2.1] and [14, Lemma 5.1]. To begin, we recall from above that for any g relatively prime to the elements of S and any c relatively prime to g,

$$\pi(x, g, c) \ge \frac{x}{2\phi(g)\log x}.$$

By Montgomery and Vaughan's explicit version of the Brun–Titchmarsh theorem [11], we also know that

$$\pi(x, g, c) \le \frac{2x}{\phi(g)\log x}.$$

To count all of the primes q less than x for which $q = gl + 1$ with $g|J$ and $l \le x^{1-B}$, consider

$$\begin{aligned}\sum_{g|J} \pi(gx^{1-B}, g, 1) &\ge \sum_{g|J}\Big[\pi(gx^{1-B}, g, 1) - \sum_{g'|J/g} \pi(gx^{1-B}, g'g, 1)\Big] \\ &\ge \frac{gx^{1-B}}{2\phi(g)\log x} - \sum_{g'|J/g} \frac{2gx^{1-B}}{\phi(gg')\log x},\end{aligned}$$

where the second summand on the first line ensures that primes are not double-counted. Clearly, $\sum_{g'|J} 1/\phi(g')$ can be bounded by $\frac{1}{8}$ since z is large. So the above is

$$\begin{aligned}&\ge \sum_{g|J} \frac{gx^{1-B}}{2\phi(g)\log x} - \frac{gx^{1-B}}{4\phi(g)\log x} \\ &\ge \sum_{g|J} \frac{gx^{1-B}}{4\phi(g)\log x} \\ &\ge \sum_{g|J} \frac{x^{1-B}}{4\log x} \\ &\ge \frac{x^{1-B}}{4\log x} 2^{(1-\epsilon)z/\log z}\end{aligned}$$

where the last line is simply a count of the number of divisors of J.

Again, since z is large,

$$\frac{x^{1-B}}{4\log x} 2^{(1-\epsilon)z/\log z} \ge x^{1-B} 2^{z/(2\log z)}.$$

Since there are x^{1-B} choices for l between 1 and x^{1-B}, we know by the pigeonhole principle that there must exist an l with at least $2^{z/(2\log z)}$ primes. Let us denote this l by l_0. Then, as required,

$$|Q_{l_0}| \ge 2^{z/(2\log z)}.$$

This concludes the proof. □

https://doi.org/10.1017/S0004972719000133 Published online by Cambridge University Press

Note that while the proof above is roughly the same as the one in [1] or [14], we use it here for different purposes. In the cited works, this result is used to generate primes p that can be combined into Carmichael numbers. In our case, we use this theorem one step earlier; it allows us to create an L that we will then use to find these primes p.

We also remark here that we can give a very trivial upper bound for $|Q_{l_0}|$ by noting that Q_{l_0} can have at most $\omega(J)$ elements, where $\omega(J)$ is the number of prime divisors of J. So

$$|Q_{l_0}| \leq 2^{2z/\log z}.$$

6. Constructing L

Next, we follow the more standard framework of constructing the prime factors of the Carmichael numbers themselves. Having now found our choices for q, we multiply them together into a large L (with small $\lambda(L)$). From here, we will find primes of the form $p = dk + 1$, where $d|L$.

To begin, let us define

$$L = \prod_{q \in Q_{l_0}} q.$$

Let $\lambda(n)$ denote the maximum order of an element (mod n). We prove the following estimate for $\lambda(L)$.

Lemma 6.1. *For $\lambda(L)$ as defined above,*

$$\lambda(L) \leq e^{3z}.$$

Proof. Note that every prime divisor q of L is such that $(q-1)|Jl$. By construction, $l < x^{1-B} < J^{7/5}$. Recall also that the product of primes up to z can be bounded by $e^{1.02z}$, according to [12, Theorem 9]. So

$$\lambda(L) \leq \Bigg[\prod_{r \text{ prime},\ r<z} r \Bigg]^{12/5} \leq e^{3z}.$$

This concludes the proof. □

7. Constructing the tuple

We can now finally define our tuple. Let

$$D(y) = \{2dy + 1 : d|L\}.$$

The goal of the rest of the paper will then be to prove that, assuming Conjecture 3, this tuple will (for infinitely many choices of y) give enough primes relative to $\lambda(L)$ such that some product of these primes will yield a Carmichael number. Obviously, the number of prime factors of each of these Carmichael numbers must then be less than the size of the tuple, thereby proving the theorem.

https://doi.org/10.1017/S0004972719000133 Published online by Cambridge University Press

More specifically, let us define $n(L)$ to be the smallest number such that a collection of at least $n(L)$ elements (mod L) must contain some subset whose product is the identity. To prove the main theorem from here, we will need to show that $|D|$ is large and $n(L)$ is small.

LEMMA 7.1. *For D as above,*

$$|D| \geq 2^{2^{z/(2\log z)}}.$$

PROOF. This follows trivially from the fact that D is comprised of every possible (nonempty) combination of elements in Q_l, where $Q_l \geq 2^{z/(2\log z)}$. □

For ease of comparison, we will say that

$$|D| \geq e^{e^{z/(4\log z)}}. \tag{7.1}$$

We also need a result about $n(L)$. To this end, we cite the following theorem which appears in [5] and [10].

THEOREM 7.2. *For $n(L)$ as above,*

$$n(L) \leq \lambda(L)\Big(1 + \frac{\log|L|}{\lambda(L)}\Big).$$

In fact, we can even be more specific about the number of elements that we are multiplying together to get the identity. The following theorem appears in [1, Proposition 1.2].

THEOREM 7.3. *Let $s > t > n = n(L)$ be integers. Then any sequence of s elements (mod L) contains at least*

$$\binom{r}{t}\Big/\binom{r}{n}$$

distinct subsequences of length at most t and at least $t - n$ whose product is the identity.

We can combine these two theorems with Lemma 6.1 to find a bound for $n(L)$.

LEMMA 7.4. *We have $n(L) \leq e^{5z}$.*

PROOF. From Lemma 6.1,

$$\lambda(L) \leq e^{3z}.$$

Since the number of primes that are multiplied to form L is $|Q_{l_0}|$ and the size of each prime is at most Jl,

$$L \leq (Jl + 1)^{|Q_{l_0}|} \leq e^{3z \cdot 2^{2z/\log z}}.$$

This implies that $\log L \leq e^{2z}$, which means that

$$n(L) \leq \lambda(L)\Big(1 + \frac{\log|L|}{\lambda(L)}\Big)e^{3z} \leq e^{5z},$$

concluding the proof. □

https://doi.org/10.1017/S0004972719000133 Published online by Cambridge University Press

8. Completing the proof

We can now invoke Conjecture 3 to prove the existence of R as required in the Main Theorem. First, we prove that for a given z, we can find an appropriate R.

THEOREM 8.1. *Assume the even weaker version of Dickson's k-tuple Conjecture (Conjecture 3) as stated in Section 3. Then there are infinitely many Carmichael numbers with exactly R prime factors, where* $e^{7z} < R < e^{8z}$.

PROOF. Let $m = e^{10z}$. By Conjecture 3, any k-tuple with $k \geq e^{e^{10z/\log^T(10z)}}$ must be such that at least m of the forms in the tuple are simultaneously prime infinitely often. From (7.1), we know that $|D|$ is greater than this choice of k. So there must exist infinitely many y such that, for each of these y, there are m terms in the tuple which are simultaneously prime.

Now, choose a y such that there are at least m primes in the tuple. We will apply Theorem 7.3. Let $s = e^{10z}$ and $t = e^{8z}$. Since $n \leq e^{5z}$, we know that $t - n \geq e^{7z}$. So by Theorem 7.3, for this choice of y, there exist subsets of these m primes whose product is 1 (mod L). Let $p_1, p_2, \ldots, p_s$ denote such a set of primes and define c to be their product. Since

$$c = p_1 p_2 \cdots p_s \equiv 1 \pmod{Ly}$$

and $(p_i - 1) | Ly$ for every i, we know that $(p_i - 1) | (c - 1)$ for every $p_i | c$. Thus, c is a Carmichael number; more specifically, c is a Carmichael number with between $t - n$ and t factors.

Since there are infinitely many choices of y, there are infinitely many Carmichael numbers with between $t - n$ and t factors. □

Finally, we prove the Main Theorem. Let us restate it here.

MAIN THEOREM. Assume the even weaker version of Dickson's k-tuple Conjecture (Conjecture 3). Let $C_R(x)$ denote the number of Carmichael numbers up to x with exactly R prime factors. Then there are infinitely many R for which $C_R(x)$ goes to infinity as x goes to infinity.

PROOF. Theorem 8.1 above states that for any sufficiently large z, we can find an R with $e^{7z} \leq R \leq e^{8z}$ such that there are infinitely many Carmichael numbers with exactly R prime factors. Since there are infinitely many choices for z, there are infinitely many such R, thereby proving the Main theorem. □

Acknowledgement

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

https://doi.org/10.1017/S0004972719000133 Published online by Cambridge University Press

References

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

[2] R. C. Baker and W. M. Schmidt, 'Diophantine problems in variables restricted to the values 0 and 1', *J. Number Theory* **12**(4) (1980), 460–486.

[3] J. Chernick, 'On Fermat's simple theorem', *Bull. Amer. Math. Soc. (N.S.)* **45** (1935), 269–274.

[4] R. D. Carmichael, 'Note on a new number theory function', *Bull. Amer. Math. Soc. (N.S.)* **16** (1910), 232–238.

[5] P. Van Emde Boas and D. Kruyswijk, 'A combinatorial problem on finite Abelian groups', in: *Afdeling Zuivere Wisk*, Vol. 3 (Math. Centrum, Amsterdam, 1969).

[6] P. Erdős, 'On pseudoprimes and Carmichael numbers', *Publ. Math. Debrecen* **4** (1956), 201–206.

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

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

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

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

[11] H. L. Montgomery and R. C. Vaughan, 'The large sieve', *Mathematika* **20** (1973), 119–134.

[12] J. B. Rosser and L. Schoenfeld, 'Approximate formulas for some functions of prime numbers', *Illinois J. Math.* **6** (1962), 64–94.

[13] T. Wright, 'Factors of Carmichael numbers and a weak k-tuples conjecture', *J. Aust. Math. Soc.* **100**(3) (2016), 421–429.

[14] T. Wright, 'There are infinitely many elliptic Carmichael numbers', *Bull. London Math. Soc.* **50**(5) (2018), 791–800.

THOMAS WRIGHT, 429 N. Church St., Spartanburg,
SC 29302, USA
e-mail: WrightTJ@wofford.edu

https://doi.org/10.1017/S0004972719000133 Published online by Cambridge University Press