



CARMICHAEL NUMBERS WITH A SPECIFIED NUMBER OF PRIME FACTORS

Daniel Larsen

Massachusetts Institute of Technology, Cambridge, Massachusetts
dlarsen@mit.edu

Thomas Wright

Department of Mathematics, Wofford College, Spartanburg, South Carolina
wrighttj@wofford.edu

Received: 10/1/25, Accepted: 6/8/26, Published: 9/28/26

Abstract

We prove that for every sufficiently large integer R , there exists a Carmichael number with exactly R prime factors.

– To Carl Pomerance on his 80th birthday

1. Introduction

A natural number n is said to be *Carmichael* if $a^n \equiv a \pmod{n}$ for every integer a . Korselt's criterion [5] tells us that a square-free composite number n is Carmichael if and only if $p - 1 \mid n - 1$ for every prime p dividing n .

Alford, Granville, and Pomerance [1] proved in 1994 that there exist infinitely many Carmichael numbers. Moreover, it is known [2] that for every R between 3 and 10^{10} , there exist Carmichael numbers with precisely R prime factors. Granville and Pomerance [4] have conjectured that for every $R \geq 3$, there are $x^{1/R+o(1)}$ Carmichael numbers less than x with exactly R prime factors, a conjecture that seems far out of reach of modern methods.

In this paper, we will prove the following weaker form of this conjecture.

Theorem 1. *For all sufficiently large R , there exist Carmichael numbers with precisely R prime factors.*

Such a result was previously known only under the assumption of Dickson's prime k -tuples conjecture [3]. Our result establishes unconditionally that there exist infinitely many Carmichael numbers with a prime number of prime factors,

strengthening a result of the second author [9] which showed this to be true under the assumption of a conjecture of Heath-Brown regarding the first prime in an arithmetic progression.

The traditional Alford–Granville–Pomerance method for producing infinite families of Carmichael numbers is based on constructing a set of primes $\mathcal{P}$ along with positive integers k and L such that:

- $k \mid p - 1$ for every $p \in \mathcal{P}$;
- $\frac{p-1}{k} \mid L$ for every $p \in \mathcal{P}$;
- $\lambda(L)$, the maximum order of an element in $(\mathbb{Z}/L\mathbb{Z})^\times$, is small compared to $|\mathcal{P}|$;
- k and L are relatively prime.

One then studies the distribution of randomly chosen products of elements of $\mathcal{P}$ modulo L . Essentially, because of the absence of large cyclic subgroups of $(\mathbb{Z}/L\mathbb{Z})^\times$, it can be shown that with probability at least $1/\phi(L) - \epsilon$, such a product is congruent to 1 modulo L . Let Π be such a product. Then $\Pi \equiv 1 \pmod{L}$, but since each of its prime factors has the form $dk+1$ for some integer d , it is also true that Π is congruent to 1 $\pmod{k}$. Since k and L are relatively prime, $\Pi \equiv 1 \pmod{Lk}$. Finishing off the argument, every prime factor $p = dk + 1$ of Π satisfies $p - 1 \mid dk \mid Lk \mid \Pi - 1$. Hence Π is a Carmichael number.

This proof relies on the size of $\mathcal{P}$ being large compared to $\lambda(L)$, but in fact, we can decompose $\mathcal{P}$ into many disjoint subsets, each of which is still large compared to $\lambda(L)$. It is easy to see that if we pick one Carmichael number obtained from each subset, we obtain a large set of Carmichael numbers such that all products obtained by multiplying distinct elements from this pool are themselves Carmichael. The basic point here is that the product of numbers congruent to 1 mod L is itself 1 mod L . This story can be found in [1], and one conclusion is that the set $\{\omega(n) : n \text{ Carmichael}\}$ has some additive structure.

Our argument begins with the observation that for such $\mathcal{P}$, we can produce long sequences of Carmichael numbers, each of which is formed from the previous one by multiplying in h additional prime factors, for some positive integer h . For instance, h could be the most frequent number of prime factors for the Carmichael numbers in our pool. The challenge then becomes showing that for arbitrary $a \bmod h$, we can construct Carmichael numbers from $\mathcal{P}$ with $a \bmod h$ prime factors. To do this, we will use methods similar to [6]. All that then remains is to show that we can fuse these two constructions to cover every number of the form $a + bh$ with b in a reasonable range, which is to say, cover every number in a large interval. Repeating this construction with larger sets $\mathcal{P}$, we obtain overlapping sets of integers covered by our construction going out to infinity.

It will turn out that because $(\mathbb{Z}/L\mathbb{Z})^\times$ has a terrifyingly large number of subgroups of index 2, we will have some additional difficulties in producing Carmichael numbers with an odd number of prime factors. The issue of handling index 2 subgroups is a well-known obstruction in the study of Carmichael numbers - see, for instance, the difference between the lower bounds in [7] and [8]. However, our specific construction cannot use the techniques of [8] without taking x , the parameter which controls the size of the prime factors of our Carmichael numbers, infeasibly large in terms of the base parameter y . The solution is to instead fix a prime factor like 3 and try to arrange for the number of prime factors added on to produce a Carmichael number to be even, which can be done quite naturally.

We will begin by recalling the machinery of [6], then stepping back temporarily to recall some key ideas underlying the machinery, and adapting them to suit our particular needs. This will be sufficient to prove that all sufficiently large even numbers are represented by values of ω on Carmichael numbers. Finally, we will reengage with the full machinery to complete the proof.

2. Notation and Terminology

We use a combination of Vinogradov notation and O -notation, at times preferring the flexibility of the latter, which allows for expressions such as $x^{1-o(1)}$, which represents a quantity larger than $x^{1-\epsilon}$ for any fixed $\epsilon > 0$, for sufficiently large x .

We say *almost none* of the elements in a set $\mathcal{S}$ have a property if the number of elements with the property is $o(|\mathcal{S}|)$. Conversely, *almost all* the elements have a property if almost none of the elements satisfy the negation of the property.

We let $\phi(n)$ represent *Euler's totient function*, defined as the number of units in the ring $\mathbb{Z}/n\mathbb{Z}$, and $\lambda(n)$ represent *Carmichael's lambda function*, defined as the smallest positive m for which $a^m \equiv 1 \pmod{n}$ for all $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. We also define $\omega(n)$ to be the number of distinct prime factors of n .

3. Establishing Equidistribution

We begin by summarizing the construction which occupies the first seven sections of [6]. Let $\mathcal{A}(x)$ be the collection of sets of positive integers $\mathcal{A}$ such that

$$\log(\max \mathcal{A}) / \log |\mathcal{A}| = O(1)$$

and

$$x < |\mathcal{A}| = \exp(x^{o(1)}).$$

Definition 1. An increasing divergent sequence of positive numbers $x_1, x_2, \dots$ is

said to be *logarithmically dense* if for every $\epsilon > 0$, there exists i such that for all $j \geq i$, we have $\log x_{j+1} - \log x_j < \epsilon$.

Proposition 1. *There exists a logarithmically dense sequence of positive numbers x , each with the property that there exist positive integers L_1 and L_2 such that for any maps $\phi_1, \phi_2 : \mathbb{N} \rightarrow \mathcal{A}(x)$, there exist positive integers k_1 and k_2 as well as sets of primes $\mathcal{P}_1$ and $\mathcal{P}_2$ such that for some choice $A_1 \in \phi_1(k_1)$ and $A_2 \in \phi_2(k_2)$, the following properties are satisfied:*

- (i) $k_1, k_2 \leq x$;
- (ii) k_1 and k_2 are divisible by 2 but not by 3 or 4;
- (iii) $k_1 k_2$ is relatively prime to $L_1 L_2$;
- (iv) L_1 is relatively prime to L_2 ;
- (v) $\gcd(\phi(L_1), \phi(L_2))$ is a power of 2;
- (vi) $\gcd(\phi(k_i), \phi(L_j))$ is a power of 2 for any choice of $i, j \in \{1, 2\}$;
- (vii) $\max_{p|k_1 k_2 L_1 L_2} \text{ord}_2(p-1) = O(1)$;
- (viii) 3 is a quadratic residue modulo L_1 and L_2 ;
- (ix) $\lambda(L_1)$ and $\lambda(L_2)$ are not divisible by 4;
- (x) Every element in $\mathcal{P}_1$ has the form $dk_1 + 1$ where d divides L_1 ;
- (xi) Every element in $\mathcal{P}_2$ has the form $dk_2 + 1$ where d divides L_2 ;
- (xii) $\lambda(L_1 L_2) = |\mathcal{P}_1|^{o(1)}$ and $\lambda(L_1 L_2) = |\mathcal{P}_2|^{o(1)}$;
- (xiii) $\log |\mathcal{P}_1| \gg \log x$ and $\log |\mathcal{P}_2| \gg \log x$;
- (xiv) For every prime q dividing $L_1 L_2$, the asymptotic $\log q \ll \log \log x$ holds;
- (xv) For every non-principal character χ modulo k_2 , for any z , there are at least $|\mathcal{P}_1|/\log x$ elements $p \in \mathcal{P}_1$ for which $\chi(p) \neq z$;
- (xvi) For every non-principal character χ modulo k_1 , for any z , there are at least $|\mathcal{P}_2|/\log x$ elements $p \in \mathcal{P}_2$ for which $\chi(p) \neq z$;
- (xvii) For any set of $\lfloor k_2/(\log x \log \log x) \rfloor$ residues modulo k_2 , almost none of the integers which can be written as a product of 10 elements from $\mathcal{P}_1$ have modulo k_2 residue in that set;

- (xviii) For any set of $\lfloor k_1/(\log x \log \log x) \rfloor$ residues modulo k_1 , almost none of the integers which can be written as a product of 10 elements from $\mathcal{P}_2$ have modulo k_1 residue in that set;
- (xix) Almost none of the elements of $\mathcal{P}_1$ are contained in any specific odd-order coset of $(\mathbb{Z}/L_2\mathbb{Z})^\times$;
- (xx) Almost none of the elements of $\mathcal{P}_2$ are contained in any specific odd-order coset of $(\mathbb{Z}/L_1\mathbb{Z})^\times$;
- (xxi) $3A_1$ has odd order modulo k_2 ;
- (xxii) $3A_2$ has odd order modulo k_1 .

In this paper, we will need a construction which avoids many of the difficulties of Proposition 1 while at the same time having a slightly stronger equidistribution hypothesis. We will quickly build up the modified construction, beginning by introducing the following definition.

Definition 2. A sequence $a_1, \dots, a_k$ of positive numbers is said to be *logarithmically spread* if $1 + 1/1000 \leq \log a_{i+1}/\log a_i \leq 10$ for every $i < k$.

Now we have the following proposition, combining Proposition 3 and Lemma 10 of [6] and taking $y_1 = y^\rho$, $y_2 = y^\theta$, $y_3 = y^{\theta(1+\iota)}$, $y_4 = y^{\theta+\rho-\iota}$, $y_5 = y$, and $w = \lfloor y^{\theta+\iota\rho} \rfloor$. (Recall that in that paper, ι is a small constant (for concreteness, let us specify $\iota = 1/1000$), $\rho = 1/24 - 2\iota$, and $\theta = 1/6 - 2\iota$.)

Proposition 2. For every large integer y_5 , there exist positive numbers y_1, y_2, y_3 , and y_4 as well as a positive integer w and a positive square-free integer L such that the following hold:

- The sequence $y_1, y_2, w, y_3, y_4, y_5$ is logarithmically spread;
- $y_2 = y_5^{1/6-1/500}$;
- $\omega(L) \geq y_4$;
- Every prime q dividing L satisfies $q \leq y_5$;
- $q - 1$ is square-free for every prime q dividing L ;
- Defining $L_{(p)}$ to be the product of those primes q with $p \mid q - 1$ and $q \mid L$, the value $L_{(p)}$ is greater than one only for $p \in [y_3, y_5]$ or $p = 2$;
- For every $p > 2$, $\omega(L_{(p)}) \leq y_1$;
- The number of primes p with $L_{(p)} > 1$ is $O(y_2)$;

- 3 is a quadratic residue modulo L ;
- Taking $\mathcal{D}$ to be the set of divisors of L with w prime factors,

$$\#\{d \in \mathcal{D} : d \equiv a \pmod{L_{(p)}}\} = \frac{|\mathcal{D}|}{\phi(L_{(p)})}(1 + o(1)) \quad (1)$$

for each residue class $a \in (\mathbb{Z}/L_{(p)}\mathbb{Z})^\times$ for every odd prime p with $L_{(p)} > 1$.

Remark 1. Roughly speaking, this proposition demonstrates how L_1 and L_2 are constructed in Proposition 1. From there, k_i are chosen to make

$$\mathcal{P}_i = \{dk_i + 1 \in \mathbb{P} : d \mid L_i\}$$

large.

Note that, using q to represent primes as we do throughout,

$$\sum_{q \mid L} \frac{1}{q} \leq \sum_{\substack{p > 2 \\ L_{(p)} > 1}} \sum_{\substack{q \equiv 1 \pmod{p} \\ q \in [y_3, y_5]}} \frac{1}{q} \ll \sum_{\substack{p > 2 \\ L_{(p)} > 1}} \frac{\log \log y_5 - \log \log y_3}{p} \ll \frac{y_2}{y_3} = o(1), \quad (2)$$

which in particular means that almost all integers less than L are units modulo L .

Let $s = y_1^2$. Let k be a fixed integer relatively prime to L . Fix an odd prime p with $L_{(p)} > 1$, let $G = (\mathbb{Z}/L_{(p)}\mathbb{Z})^\times$, and let G' be a coset of index p . Consider ϵ_j , the probability that $d_1k + 1, \dots, d_jk + 1 \in G'$ where each d_i is chosen uniformly and independently from $\mathcal{D}$. If t distinct elements of $\mathcal{D}$ are represented among the d_i , the probability that $\{d_ik + 1\}$ are all in G' is ϵ_1^t . Now,

$$\epsilon_s < \sum_{t=1}^s \epsilon_1^t \binom{|\mathcal{D}|}{t} \frac{t^s}{|\mathcal{D}|^s} < \sum_{t=1}^s (\epsilon_1 e)^{-s} \left(\frac{t}{|\mathcal{D}| \cdot (\epsilon_1 e)} \right)^{s-t} \ll (\epsilon_1 e)^{-s}.$$

By Equations 1 and 2, $\epsilon_1 = \frac{1}{p}(1 + o(1))$. Thus,

$$\epsilon_s = (O(1/p))^s \leq y_3^{-s(1-o(1))}$$

Note that G contains $p \cdot \frac{p^{\text{rank}_p(G)} - 1}{p - 1}$ cosets of index p . Recall that $\omega(L_{(p)}) \leq y_1$. Thus, the probability that any G' exists is bounded by

$$\underbrace{y_3^{-s(1-o(1))}}_{\text{probability for single coset}} \cdot \underbrace{y_5^{O(y_1)}}_{\text{number of cosets for fixed } p} \cdot \underbrace{y_5}_{\text{number of choices of } p}.$$

That is, the probability that $d_1k + 1, \dots, d_s k + 1$ all lie in a proper coset of $(\mathbb{Z}/L\mathbb{Z})^\times$ of odd index is bounded by

$$y_3^{-s(1-o(1))}. \quad (3)$$

4. Finding Primes

Let $\pi(x; q, a)$ count the number of primes up to x congruent to $a \bmod q$. As in [1], for $B = 1/3$, it holds for sufficiently large x that

$$\pi(dx; d, 1) \geq \frac{\pi(dx)}{2\phi(d)}$$

for every $d \leq x^B$ not containing a divisor in some exceptional set $\mathcal{D}_B(x)$ of bounded size. Set $x = y_5^{\frac{w}{1/6-3/1000}}$. This choice is simply to maintain compatibility with [6]; the important thing is that every $d \in \mathcal{D}$ is less than x^B . Let $\mathcal{D}'$ be the subset of $\mathcal{D}$ consisting of those elements which are divisible by none of the elements in $\mathcal{D}_B(x)$. Since $w = o(\omega(L))$, we have $|\mathcal{D}'| = |\mathcal{D}|(1 - o(1))$. For fixed $d \in \mathcal{D}'$, let $\mathcal{K}_d$ be the set of $k < x$ with $dk + 1$ prime. We then have

$$|\mathcal{K}_d| = \pi(dx; d, 1) > \frac{x}{3 \log x}.$$

Indeed,

$$\frac{\phi(d)}{d} \geq \frac{\phi(L)}{L} = 1 - o(1)$$

by Equation (2). Now, for each prime q dividing L , the number of k divisible by q in $\mathcal{K}_d$ is

$$\pi(dx; dq, 1) < \frac{3dx}{\log x \cdot \phi(dq)} < \frac{4x}{\log x \cdot q}$$

by the Brun-Titchmarsh theorem. Therefore, the number of $k \in \mathcal{K}_d$ relatively prime to L is greater than

$$\frac{x}{3 \log x} - 4 \sum_{q|L} \frac{x}{\log x \cdot q} > \frac{x}{4 \log x}$$

by Equation (2).

Let $\tilde{\mathcal{K}}$ be the set of $k \leq x$ for which there exists a proper odd-order coset of $(\mathbb{Z}/L\mathbb{Z})^\times$ containing $dk + 1$ for at least $|\mathcal{D}|/(\log x \log \log x)$ values of $d \in \mathcal{D}'$. Then there exist $|\tilde{\mathcal{K}}| \cdot (|\mathcal{D}|/(\log x \log \log x))^s$ choices of $k \leq x$ and $d_1, \dots, d_s \in \mathcal{D}'$ (where repeats are allowed and order matters) with all of $\{d_i k + 1\}_i$ in some proper coset. However, by Equation (3), there are at most $x|\mathcal{D}|^s/y_3^{s(1-o(1))}$ such choices with that property. Hence

$$|\tilde{\mathcal{K}}| < \frac{x(\log x \log \log x)^s}{y_3^{s(1-o(1))}} = x \left(\frac{\log x \log \log x}{y_3^{1-o(1)}} \right)^s$$

and since $\log x \ll w \log y_5$, this quantity is far smaller than, for instance, $x/\log^2 x$.

Let

$$\mathcal{K}'_d = \{k \in \mathcal{K}_d : k \notin \tilde{\mathcal{K}}, (k, L) = 1, k > \sqrt{x}\}.$$

We have shown that $|\mathcal{K}'_d| \geq x/(5 \log x)$. By the pigeonhole principle, there exists a specific value $k \in \mathcal{K}'_d$ such that there are at least $|\mathcal{D}|/(5 \log x)$ primes of the form $dk + 1$ with $d \in \mathcal{D}'$. Let $\mathcal{P}$ be this set.

Note that this construction, performed twice with separate values of L and k and some careful bookkeeping which can be found in [6], is enough to recover most of Proposition 1. The most delicate component is properties (xv)–(xviii), but Section 7 of [6] shows that these hold generically in some sense.

5. Producing Carmichael Numbers

The Davenport constant for a finite abelian group G is the smallest integer n for which any sequence of n elements of G contains a non-empty subsequence whose product is equal to the identity.

We will need the following bound about the Davenport constant, adapted from Theorem 2 of [1].

Proposition 3. *Let n be the Davenport constant of $(\mathbb{Z}/L\mathbb{Z})^\times$. Then*

$$n \leq \lambda(L)(1 + \log(|L|/\lambda(L))) + 1.$$

We will also need Proposition 7 from [6].

Proposition 4. *Let G be a finite abelian group, let $g \in G$, and let n be such that for any sequence of n elements of G , there is a non-empty subsequence whose product is 1. Suppose $r > t > n$. Suppose S is a sequence of length r whose terms multiply to g . Then there are at least $\binom{r}{t} \binom{r}{n}^{-1}$ subsequences of S of length at most t whose product is g .*

By definition of n being the Davenport constant of $(\mathbb{Z}/L\mathbb{Z})^\times$, for any sequence of n elements of $\mathcal{P}$, there is a sub-product congruent to 1 modulo L . Hence, there exists $h_0 \leq n$ such that with probability at least $1/n$, for a randomly chosen set of primes taken from $\mathcal{P}$, there is a sub-product of length h_0 congruent to 1 modulo L .

Note that

$$\lambda(L) = \prod_{p: L(p) > 1} p = y_5^{O(y_2)}$$

whereas

$$|\mathcal{P}| \gg \binom{\omega(L)}{w} \cdot (\log x)^{-1} > y_5^{\epsilon w}$$

for some absolute constant $\epsilon > 0$. Consequently,

$$\log |\mathcal{P}| \gg \log x$$

and there exist many integers r such that

$$\log \lambda(L) / \log r = o(1), \quad \log r / \log |\mathcal{P}| = o(1). \quad (4)$$

Proposition 5. *Let L and r be positive integers, and let $\mathcal{P}$ be a set of primes such that Equation (4) holds. Suppose that $q-1$ is square-free for every prime q dividing L and that L is odd. Suppose further that for any specific coset of $(\mathbb{Z}/L\mathbb{Z})^\times$ of odd order, $o(|\mathcal{P}|)$ elements of $\mathcal{P}$ are contained in that coset. Let $a \bmod h$ be any arithmetic progression containing even numbers with $h \ll \lambda(L)^2$. For any quadratic residue $\square \bmod L$, and for almost all r -element subsets $\mathcal{P}^\star \subset \mathcal{P}$, there exists a square-free positive integer N with the following properties:*

- $N > 1$;
- All prime factors of N are in $\mathcal{P}^\star$;
- $N \equiv \square \pmod{L}$;
- $\omega(N) \equiv a \pmod{h}$;
- $\omega(N)$ is even.

Proof. We may assume that a and h are even without loss of generality. Indeed, we may multiply them by two if not.

For any finite abelian group, the number of maximal odd-order proper cosets is less than twice the order. Even if 10% of the elements of $\mathcal{P}$ were contained in a maximal odd-order coset of $(\mathbb{Z}/L\mathbb{Z})^\times$ (a far larger fraction than could truly be the case), the probability that the majority of the elements of $\mathcal{P}^\star$ would be in the coset is

$$10^{-r/2} \binom{r}{\lceil r/2 \rceil} < 5^{-r/2}$$

which by Equation (4) is far smaller than $1/L$. Therefore, for the rest of the proof, we may assume that for any odd-order coset of $(\mathbb{Z}/L\mathbb{Z})^\times$, the majority of the elements of $\mathcal{P}^\star$ live outside the coset.

Let g be the element $(\square, a)$ in

$$G := (\mathbb{Z}/L\mathbb{Z})^\times \oplus \mathbb{Z}/h\mathbb{Z}.$$

Let h' be the largest odd factor of h . We decompose G as $G_1 \oplus G_2 \oplus G_3 \oplus G_4$ where G_1 is the maximal subgroup of odd order in $(\mathbb{Z}/L\mathbb{Z})^\times$, $G_2 = \mathbb{Z}/h'\mathbb{Z}$, G_3 is the 2-Sylow subgroup of $(\mathbb{Z}/L\mathbb{Z})^\times$, and G_4 is the 2-Sylow subgroup of $\mathbb{Z}/h\mathbb{Z}$. Recall that $q-1$ is square-free for every prime q dividing L . Therefore, every element in G_3 other than the identity has order 2. In particular, $\square$ corresponds to 1 in G_3 .

Label the elements of $\mathcal{P}^\star$ as $p_1, \dots, p_r$ and let P be their product. We need to bound

$$\frac{|G|}{2^r} \sum_{d|P} \mathbb{1}_G(d = g) = \frac{1}{2^r} \sum_{d|P} \sum_{\chi \in \hat{G}} \overline{\chi(g)} \cdot \chi(d). \quad (5)$$

Switching the order of summation, this is equal to

$$\sum_{\substack{\chi_i \in \hat{G}_i \\ i \in \{1,2,3,4\}}} \overline{\chi_1(g)\chi_2(g)\chi_3(g)\chi_4(g)} \prod_{j=1}^r \frac{1 + \chi_1(p_j)\chi_2(p_j)\chi_3(p_j)\chi_4(p_j)}{2},$$

where p_j is viewed as the element $(p_j \bmod L, 1)$ (according to the original description of G). We note that the groups G_2 and G_4 are additive, and hence 1 is not the identity in either of these groups. Let $*(\chi)$ be the condition that

$$\chi_1(p_j)\chi_2(p_j)\chi_3(p_j)\chi_4(p_j) = 1$$

for the majority of p_j . We may break our sum over characters as follows:

$$\sum_{\substack{\chi_i \in \hat{G}_i \\ i \in \{1,2,3,4\} \\ *(\chi)}} \overline{\chi_1(g)\chi_2(g)\chi_3(g)\chi_4(g)} \prod_{j=1}^r \frac{1 + \chi_1(p_j)\chi_2(p_j)\chi_3(p_j)\chi_4(p_j)}{2} + O(\epsilon|G|),$$

where ϵ is the largest value of

$$\left| \prod_{j=1}^r \frac{1 + \chi_1(p_j)\chi_2(p_j)\chi_3(p_j)\chi_4(p_j)}{2} \right|$$

for characters not satisfying $*(\chi)$.

Write $H_1 = G_1$, $H_2 = G_2$, and $H_3 = G_3 \oplus G_4/2G_4$. Since $*(\chi)$ is certainly not true if χ_4 has order greater than two, Equation (5) is equal to

$$\sum_{\substack{\chi_i \in \hat{H}_i \\ i \in \{1,2,3\} \\ *(\chi)}} \overline{\chi_1(g)\chi_2(g)\chi_3(g)} \prod_{j=1}^r \frac{1 + \chi_1(p_j)\chi_2(p_j)\chi_3(p_j)}{2} + O(\epsilon|G|).$$

By our coset discussion from earlier, if χ_1 is not principal then $*(\chi)$ is not satisfied because $\chi_2(p_j)$ does not depend on j and the condition $*(\chi)$ requires $\chi_1(p_j)\chi_2(p_j) = 1$ for most j . Once χ_1 is taken to be principal, this requirement tells us that for $*(\chi)$ to be satisfied, we also need χ_2 to be principal. Therefore, Equation (5) equals

$$\sum_{\substack{\chi_3 \in \hat{H}_3 \\ *(\chi)}} \overline{\chi_3(g)} \prod_{j=1}^r \frac{1 + \chi_3(p_j)}{2} + O(\epsilon|G|).$$

Since $\chi_3(g) = 1$, Equation (5) equals

$$\sum_{\substack{\chi_3 \in \hat{H}_3 \\ *(\chi)}} \prod_{j=1}^r \frac{1 + \chi_3(p_j)}{2} + O(\epsilon|G|).$$

The main term is equal to a constant $|H_3|/2^r$ times the number of divisors of P corresponding to the identity as an element of H_3 . Proposition 4 tells us that the number of such divisors is quite large, certainly larger than $2^r/e^{-\lambda(L)^2}$, whereas

$$\epsilon < (1 - \lambda(L)^{-7})^{r/2} < e^{-\sqrt{r}}.$$

In particular, Equation (5) has positive real part, and there must exist N satisfying our conditions. $\square$

We need one more important tool, of a combinatorial nature.

Lemma 1. *Let $\mathcal{P}$ be a set of primes and M be an integer such that $p - 1 \mid M$ for every $p \in \mathcal{P}$. Let r be a positive integer such that $|\mathcal{P}| \geq r^4$. Suppose N is congruent to 1 mod M and comprised of at most $10r$ distinct primes in $\mathcal{P}$. Finally, suppose h is such that a randomly chosen r -element subset of $\mathcal{P}$ contains a sub-product of length h congruent to 1 mod M with probability greater than or equal to $1/r$. Then for every integer in the range $[\omega(N), r^2]$ congruent to $\omega(N) \bmod h$, there exists a Carmichael number with exactly that many prime factors.*

Proof. Let $\tilde{\mathcal{P}}_0$ consist of the prime factors of N . Since r^3 is small compared to the size of $\mathcal{P}$, for any r randomly chosen primes from $\mathcal{P}$, the probability of our chosen set of primes meeting $\tilde{\mathcal{P}}_0$ is less than $1/r$. Therefore, there exists a number congruent to 1 mod M with h prime factors, all of which are contained in $\mathcal{P} \setminus \tilde{\mathcal{P}}_0$.

Define the product of these h primes to be N_1 . We add these prime factors to $\tilde{\mathcal{P}}_0$ to yield $\tilde{\mathcal{P}}_1$, and we then repeat the process to find h more primes in $\mathcal{P} \setminus \tilde{\mathcal{P}}_1$ whose product is also 1 mod M . By repeating the process as long as we can, we obtain in this way a list of numbers $N_1, \dots, N_k$, where $N \prod_{i=1}^j N_i$ is a Carmichael number for all $j \leq k$. Therefore every number in the range $[\omega(N), r^2]$ congruent to $\omega(N) \bmod h$ can be written as ω evaluated on a Carmichael number. $\square$

Let r satisfy Equation (4). Combining Proposition 5 (with $\square = 1$) and Lemma 1, we see that if h_0 is odd then every number in the range $[r, r^2]$ has a Carmichael number with that many prime factors. However, if h_0 is even, this is a priori only true for even numbers between r and r^2 . In the next section we will explain how to overcome this obstacle.

6. Constructing Carmichael Numbers With Odd Numbers of Prime Factors

We use a very simple trick, fixing 3 as a prime factor at the start. It is always easier to show that there exists a product with specified conditions with an even number of prime factors than an odd number of prime factors, and by fixing a single prime factor to begin with, we use this to our advantage.

To do this, we need to return to Proposition 1. By randomly decomposing L as $L_1 L_2$ and applying the methods of the previous three sections to separate values of L , k , and $\mathcal{P}$, we can upgrade the statement of Proposition 1 by replacing properties (xix) and (xx) with

- (xix)* Almost none of the elements of $\mathcal{P}_1$ are contained in any specific odd-order coset of $(\mathbb{Z}/L\mathbb{Z})^\times$;
- (xx)* Almost none of the elements of $\mathcal{P}_2$ are contained in any specific odd-order coset of $(\mathbb{Z}/L\mathbb{Z})^\times$.

There are a few additional properties we will need:

- (xxiii) $A_1 \equiv 1 \pmod{L_1}$ and $A_1 \equiv 3^{-1} \pmod{L_2}$;
- (xxiv) $A_2 \equiv 1 \pmod{L_2}$ and $A_2 \equiv 3^{-1} \pmod{L_1}$;
- (xxv) Every prime factor of A_1 is an element of $\mathcal{P}_1$;
- (xxvi) Every prime factor of A_2 is an element of $\mathcal{P}_2$;
- (xxvii) A_1 and A_2 each have an even number of prime factors;
- (xxviii) $A_1 A_2$ is relatively prime to $k_1 k_2 L_1 L_2$.

Let x be a value for which Proposition 1 holds, and let L_1 and L_2 be associated values. In defining ϕ_1 , it suffices to define the map on k_1 for which there exists $\mathcal{P}_1$ satisfying all the applicable properties of that proposition. For such values, take some choice of residue class $a \pmod{h}$, and take A to be one of the integers guaranteed by Proposition 5, with $\square$ corresponding to $1 \pmod{L_1}$ and $3^{-1} \pmod{L_2}$. (Note that we are allowed to apply Proposition 5 courtesy of (xix)*.) Let P be the largest square-free integer congruent to $1 \pmod{L_1 L_2}$ whose prime factors lie in $\mathcal{P}_1$ and which is prime to A . Apply Proposition 4 to the sequence of prime factors of AP with t set to be twice the Davenport constant of $(\mathbb{Z}/L_1 L_2 \mathbb{Z})^\times$. This defines a set $\phi_1(k_1)$ whose elements are congruent to $1 \pmod{L_1}$ and $3^{-1} \pmod{L_2}$. We define $\phi_2(k_2)$ analogously with indices swapped.

Proposition 6. *For any even $h \ll \lambda(L)^2$, there exist positive integers A_1 and A_2 congruent to any two specified even residues modulo h , in addition to values k_1 , k_2 , $\mathcal{P}_1$, and $\mathcal{P}_2$ such that when combined with our existing values for x , L_1 , and L_2 , these variables together satisfy properties (i)–(xxviii).*

Proof. Proposition 4 tells us that $\log |\phi_1(k_1)| \gg t \log x$. In particular, we have the bound

$$\frac{\log \max \phi_1(k_1)}{\log |\phi_1(k_1)|} = O(1).$$

We may therefore invoke Proposition 1 with properties (xxiii)–(xxviii) coming by definition of ϕ_1 . $\square$

Remark 2. This goes beyond the original construction in [6] because here h , unlike ℓ_0 , is not an $O(1)$ quantity. This is a significant difference, due to the possibility that h may share odd prime factors with $\phi(L)$. This unpleasant consideration is responsible for all the additional care that must be taken when compared with [6].

Let $L = L_1 L_2$. Let r be a positive integer with

$$\lambda(L)^{10} < r < \min(|\mathcal{P}_1|, |\mathcal{P}_2|)^{1/10}.$$

To finish off the argument, we specialize Lemma 15 from [6] to the case $w_0 = 0$ and $\ell_0 = 2$.

Lemma 2. *Subject to the properties of Proposition 1, with*

$$G := (\mathbb{Z}/L\mathbb{Z})^* \oplus (\mathbb{Z}/k_2\mathbb{Z})^* \oplus \mathbb{Z}/2\mathbb{Z},$$

for every $g \in G$ which is 1 mod L , odd order mod k_2 , and 0 mod 2, for almost all r element subsets $\mathcal{P}^ \subset \mathcal{P}_1$, there exists a product of distinct elements in $\mathcal{P}^*$ equal to g as an element of G under the map $(\cdot \bmod L, \cdot \bmod k_2, \omega(\cdot))$.*

Take g to be congruent to 1 mod L , 1 mod k_2 , and 0 mod 2. With probability 1, a subset of $\mathcal{P}_1$ of size r has a sub-product congruent to 1 mod Lk_2 with an even number of prime factors. Therefore, there exists an even $h_1 \leq r$ such that with probability at least $1/r$, a random subset of $\mathcal{P}_1$ of size r has a sub-product of length h_1 congruent to 1 mod Lk_2 .

For this value of h_1 , choose A_1 and A_2 in Proposition 6 corresponding respectively to the residues a and 0 mod h_1 , where we take a to be an arbitrary even number.

Now take g to be 1 mod L , $(3A_1)^{-1}$ mod k_2 , and 0 mod 2. Let Π_1 be one of the products guaranteed by Lemma 2, taking $\mathcal{P}^*$ disjoint from the prime factors of A_1 . Now flipping the indices, this lemma can also produce Π_2 which is congruent to 1 mod L and $(3A_2)^{-1}$ mod k_1 , while having an even number of prime factors.

Take $N = 3A_1 A_2 \Pi_1 \Pi_2$. Note that N is congruent to 1 mod L , k_1 , and k_2 , meaning in particular that N is congruent to 1 mod Lk_1 and Lk_2 . Moreover, $\omega(N)$ is congruent to $a + 1 + \omega(\Pi_1 \Pi_2)$ mod h_1 .

By Lemma 1, every number in the range $[\omega(N), r^2]$ congruent to $a + 1 + \omega(\Pi_1 \Pi_2)$ mod h_1 can be written as ω evaluated on a Carmichael number.

Since a was an arbitrary even number, every odd number in the range $[\omega(N), r^2]$ has the property that it can be written as ω evaluated on a Carmichael number. Clearly $\omega(N) \leq 4r + 1$. There exists an absolute constant c such that $\min(|\mathcal{P}_1|, |\mathcal{P}_2|) > x^c$. For every r between $x^{c/20}$ and x^c , the range $[4r + 1, r^2]$ has been covered by Carmichael prime counts. Since the sequence of valid x is logarithmically dense, we conclude that for every sufficiently large integer n , there exists a Carmichael number with exactly n prime factors.

References

- [1] W. R. Alford, A. Granville, and C. Pomerance, There are infinitely many Carmichael numbers, *Ann. of Math.* **140** (1994), 703–722.
- [2] W. R. Alford, J. Grantham, S. Hayman, and A. Shallue, Constructing Carmichael numbers through improved subset-product algorithms, *Math. Comp.* **83** (2014), 899–915.
- [3] J. Chernick, On Fermat’s simple theorem, *Bull. Amer. Math. Soc. (N.S.)* **45** (1935), 269–274.
- [4] A. Granville and C. Pomerance, Two contradictory conjectures concerning Carmichael numbers, *Math. Comp.* **71** (2002), 883–908.
- [5] A. Korselt, Problème chinois, *L’Intermédiaire des Mathématiciens* **6** (1899), 142–143.
- [6] D. Larsen, Carmichael numbers in all possible arithmetic progressions, preprint, [arXiv:2504.09056](https://arxiv.org/abs/2504.09056).
- [7] K. Matomäki, On Carmichael numbers in arithmetic progressions, *J. Aust. Math. Soc.* **94** (2) (2013), 1–8.
- [8] T. Wright, Infinitely many Carmichael numbers in arithmetic progressions, *Bull. Lond. Math. Soc.* **45** (2013), 943–952.
- [9] T. Wright, Carmichael numbers with a prime number of prime factors, *Integers* **24** (2024), #A97.