

# ON THE NUMBER OF CARMICHAEL NUMBERS UP TO $x$

GLYN HARMAN

## ABSTRACT

It is shown that, for all large  $x$ , there are more than  $x^{0.33}$  Carmichael numbers up to  $x$ , improving the ground-breaking work of Alford, Granville and Pomerance who were the first to demonstrate that there are infinitely many such numbers. The same basic construction as these authors is used, but a slight modification enables a stronger result on primes in arithmetic progressions based on a sieve method to be employed.

## 1. Introduction

A composite number  $n$  is called a *Carmichael number* if

$$n|(a^n - a) \quad \text{for all } a \in \mathbb{N}. \quad (1)$$

By Fermat's 'little theorem' all primes satisfy (1), and the existence of Carmichael numbers shows that (1) cannot be used as a reliable primality test. Indeed, (1) demonstrates that  $n|(a^{n-1} - 1)$  whenever  $(a, n) = 1$ . The latest information concerning conjectures and computational work on Carmichael numbers may be found in [8]. In [1] it was proved that there are infinitely many Carmichael numbers. Indeed, the authors proved that for all sufficiently large  $x$  the number of such integers up to  $x$  exceeded  $x^{\beta-\epsilon}$  (any  $\epsilon > 0$ ) with

$$\beta = \frac{5}{12} \left( 1 - \frac{1}{2e^{\frac{1}{2}}} \right) = 0.290306\dots > \frac{2}{7}.$$

As a corollary to the result in [2],  $\beta$  can be increased to 0.29329. It is the purpose of this paper to improve these results as follows. We henceforth write  $C(x)$  for the number of Carmichael numbers up to  $x$ .

**THEOREM 1.** *There exists  $\beta > 0.33$  such that, for all sufficiently large  $x$ , we have*

$$C(x) > x^\beta. \quad (2)$$

**REMARKS.** It is disappointing to have missed the exponent  $\frac{1}{3}$ . Our value for  $\beta$  is  $0.3322408 - \epsilon$ . It is inherent in the method that more work is likely to produce small improvements to the exponent, but even 0.3325 seems out of reach at present. It is hoped that further work on some of the ingredients used in the proof will push the lower bound for  $\beta$  past  $\frac{1}{3}$  in the next few years. In particular, the correct generalisation of [20] would lead to  $\beta > 0.334$ . The conjectured exponent is  $1 - \epsilon$  (see [8]), but we have no methods (if we use the Alford-Granville-Pomerance construction) that will give  $\beta > \frac{1}{2}$ , even if we assume the Generalised Riemann

Hypothesis. Theorem 4 in [1] gives the conjectured exponent assuming a very strong hypothesis on primes in arithmetic progressions, however.

## 2. Outline of the argument

In this paper the letter  $p$  always denotes a prime number. We shall use the same basic construction devised by Alford, Granville and Pomerance, but we shall be able to make use of a stronger result on primes in arithmetic progressions (see §3). In order to do this some of our intermediate steps will be less general than in [1]. For example, we cannot improve Theorem 3.1 of [1] as it stands, but we can give a better result for the values of the parameters that occur in the proof of Theorem 1 here. The Alford-Granville-Pomerance exponent arises as a product  $EB$ . Here  $E$  denotes a number such that, for all sufficiently large  $x$ ,

$$\sum_{\substack{p \leq x \\ P(p-1) \leq x^{1-E}}} 1 \geq \gamma_1(E)\pi(x), \quad (3)$$

where  $\gamma_1(E) > 0$ ,  $\pi(x)$  counts the number of primes up to  $x$ , and  $P(n)$  is the greatest prime factor of  $n$ . They used the value  $1 - E = (2\sqrt{e})^{-1}$  given by Friedlander [6]. Baker and Harman [2] improved this to  $1 - E = 0.2961$ , albeit with a slight weakening of the right hand side of (3) which does not damage the basic argument. The number  $B$  is such that given any  $a, q \in \mathbb{N}$  with  $(a, q) = 1, q \leq x^B$ , we have, for all sufficiently large  $x$ ,

$$\sum_{\substack{p \leq x \\ p \equiv a \pmod{q}}} 1 \geq \gamma_2(B) \frac{\pi(x)}{\phi(q)}, \quad (4)$$

where  $\gamma_2(B) > 0$ , except for relatively few exceptional  $q$ . Our adaptation of the method allows us to permit many more exceptional  $q$ , and thus increase the size of  $B$  from  $5/12 (= 0.41\bar{6})$  to  $0.472$ . The reader should note that we have kept the spirit of [1] so that all the constants we introduce here are effectively computable. Using the arguments in [1] we can therefore obtain a version of Theorem 1 with effectively computable constants for  $\beta > 0.472^2 > 2/9$ , in place of the value  $25/144 - \epsilon$  given in [1]. However, using [15, Proposition 3.2], it is possible to obtain an exponent  $> 0.2923$  with effective constants with our method (here  $1 - E = \frac{1}{2} \exp(-\frac{3}{11}) = 0.3806\dots$ ). We will be brief with details that are almost identical to [1].

## 3. Primes in Arithmetic progressions

We write  $\chi$  for a Dirichlet character, and  $L(s, \chi)$  for the corresponding L-function. As is well known, it is the possibility of zeros of  $L(s, \chi)$  near  $\operatorname{Re} s = 1$  which causes great problems for the study of primes in arithmetic progressions. The following result may have some interest in its own right. Certainly it has significant value when one can discount sufficiently many bad moduli. It replaces Section 2 of [1] in our adaptation of their argument. We write  $\pi(x; q, a)$  to denote the number of primes  $p \leq x$  with  $p \equiv a \pmod{q}$ .

THEOREM 2. *Given  $\epsilon > 0$ , there are constants  $K(\epsilon) \geq 2$  and  $c > 0$ , such that if  $q > K$  and for every  $d|q$  with  $\chi$  a primitive character (mod  $d$ ) we have*

$$L(s, \chi) \neq 0 \text{ for } \operatorname{Re} s > 1 - \frac{1}{(\log q)^{\frac{3}{4}}}, \quad |t| \leq \exp\left(\epsilon(\log q)^{\frac{3}{4}}\right), \quad (5)$$

*then, for any  $a$  with  $(a, q) = 1$ , we have*

$$\pi(x; q, a) \geq \frac{cx}{\phi(q) \log x} \quad (6)$$

*whenever  $x^{0.472} > q$ .*

REMARK. The hypothesis (5) can be weakened to

$$\operatorname{Re} s > 1 - \frac{J \log \log q}{\log q}$$

where  $J$  is another (very large) constant (and with a corresponding reduction in upper bound for  $|t|$ ), but that would make the proof more complicated without yielding any stronger results. Moreover, we could no longer say that all the arguments follow verbatim from [11].

*Proof.* The relation  $x^g > q$  is analogous to  $h > x^{1-g}$  when considering primes in intervals of the form  $[x, x+h)$ . We can obtain the result of Theorem 2 with the weaker conclusion that one requires  $x^{0.45-\epsilon} > q$  by using the method of [3]. In that paper in the application of the results one required  $q < (\log x)^A$ , although many of the intermediate results, for example Theorem 4, are stated for more general values of  $q$ . It should be noted that the parameter  $T$  there has much less significance here since we are not considering primes in short intervals. The restriction  $q < (\log x)^A$  only arose, however, to ensure a good zero free region for  $L(s, \chi)$  which led to a non-trivial bound for a Dirichlet polynomial in the argument ((3.2) in [3]). We have stipulated by (5) a sufficiently good zero-free region for the method to work.

To obtain our improved exponent we need to consider more recent work. For the problem of primes in short intervals the best result to date has  $h \geq x^{0.525}$  [4]. However, that result requires Watt's mean value result [20] which does not have an analogue in our current situation (the result in [12] cannot be applied in the present context because the parameter  $T$  has much less significance here). However, in [11] the cognate problem of the distribution of prime ideals in small regions is considered, and the exponent 0.53 is obtained, which has been sharpened to 0.528 in [16]. This is done without using any analogue of Watt's result. We will sketch the proof of Theorem 2 by showing that the arithmetical information available here is exactly analogous to that in [11] and [16]. It follows that we obtain the corresponding exponent (compare the similar argument in [14]).

Let  $\mathcal{A} = \{n \leq x : n \equiv a \pmod{q}\}$ , and write

$$S(\mathcal{A}_m, z) = \sum_{\substack{mn \in \mathcal{A} \\ p|n \Rightarrow p > z}} \left(1 - \frac{mn}{x}\right),$$

with the obvious convention that  $\mathcal{A}_1 = \mathcal{A}$ . The smoothing factor  $1 - \frac{mn}{x}$  is used for technical reasons which will become clear later. We want to show that

$$S(\mathcal{A}, x^{\frac{1}{2}}) > \frac{cx}{\phi(q) \log x}.$$

The author's sieve method (described in [9] and [10], developed in [3, 4, 11, 14]) shows how this can be done using Buchstab's identity and asymptotic formulae for sums of the form

$$\sum_{\substack{kmn \equiv a \pmod{q} \\ kmn \leq x}} a_m b_n c_k \left(1 - \frac{mnk}{x}\right) \quad (7)$$

where the coefficients  $a_m, b_n, c_k$  have a special form - indeed for some sums  $b_n \equiv 1$  (see [4], [11] for the forms which arise, and compare Lemma 2\* in [10]). Buchstab's identity in the present context gives

$$S(\mathcal{A}, x^{\frac{1}{2}}) = S(\mathcal{A}, z) - \sum_{z < p \leq x^{\frac{1}{2}}} S(\mathcal{A}_p, p),$$

where the second sum is decomposed by further applications of the identity. Asymptotic formulae can be obtained for various sums of the form

$$\sum_{m,n} a_m b_n S(\mathcal{A}_{mn}, z(mn)),$$

and Buchstab's identity is applied so that the only sums for which no such formula can be given would give a non-negative contribution. Provided that not too many of the latter type sums arise we thus obtain our desired lower bound for  $S(\mathcal{A}, x^{\frac{1}{2}})$ . The relevant details for our situation can be seen on pages 601 and 616-619 of [11].

This method can also be stated in the following form. We have

$$S(\mathcal{A}, x^{\frac{1}{2}}) \geq \sum_{n \in \mathcal{A}} \rho(n),$$

for any function  $\rho$  such that

$$\rho(n) \leq \begin{cases} 1 - n/x & \text{if } n \text{ is prime} \\ 0 & \text{if } n \text{ is composite.} \end{cases}$$

We use Buchstab's identity to construct a  $\rho$  that can be decomposed into multiple sums of the form (7). The asymptotic formulae we obtain for these give

$$\sum_{n \in \mathcal{A}} \rho(n) \sim \frac{1}{\phi(q)} \sum_{n \leq x} \rho(n).$$

The construction also ensures that

$$\sum_{n \leq x} \rho(n) > \frac{cx}{\log x},$$

and this completes the proof.

Suppose we first split the variables in (7) into ranges of the form  $M \leq m < 2M, N \leq n < 2N, K \leq k < 2K$ . We have

$$\begin{aligned} \sum_{mnk \in \mathcal{A}} a_m b_n c_k \left(1 - \frac{mnk}{x}\right) &= \frac{1}{\phi(q)} \sum_{\chi \pmod{q}} \bar{\chi}(a) \sum_{mnk \leq x} a_m b_n c_k \chi(mnk) \left(1 - \frac{mnk}{x}\right) \\ &= \frac{1}{\phi(q)} \sum_{\substack{mnk \leq x \\ (mnk, q) = 1}} a_m b_n c_k \left(1 - \frac{mnk}{x}\right) + \frac{J}{\phi(q)}, \end{aligned}$$

where

$$\begin{aligned} J &= \sum_{\substack{\chi \bmod q \\ \chi \neq \chi_0}} \bar{\chi}(a) \sum_{mnk \leq x} a_m b_n c_k \chi(mnk) \left(1 - \frac{mnk}{x}\right) \\ &= \sum_{\substack{\chi \bmod q \\ \chi \neq \chi_0}} \bar{\chi}(a) \frac{1}{2\pi i} \int_{-T}^T A(s, \chi) B(s, \chi) K(s, \chi) \frac{x^s}{s(s+1)} ds + O\left(\frac{x^{1+\epsilon}}{T^2}\right), \end{aligned}$$

with  $s = \frac{1}{2} + it$  and

$$\begin{aligned} A(s, \chi) &= \sum_{M \leq m < 2M} \chi(m) a_m m^{-s}, \quad B(s, \chi) = \sum_{N \leq n < 2N} \chi(n) b_n n^{-s}, \\ K(s, \chi) &= \sum_{K \leq k < 2K} \chi(k) c_k k^{-s}. \end{aligned}$$

In the above we have used a variant of the well-known truncated Perron formula [19, Theorem 3.12]. We can take  $T = x^{\frac{1}{2}}$  here to ensure the error in the above formula is of no consequence. We have thus reduced the problem of obtaining an asymptotic formula for (7) to showing that

$$\sum_{\substack{\chi \bmod q \\ \chi \neq \chi_0}} \int_{-T}^T |A(s, \chi) B(s, \chi) K(s, \chi)| \frac{dt}{1+|t|^2} \ll x^{\frac{1}{2}} (\log x)^{-A} \quad (8)$$

for some sufficiently large  $A$ . The purpose of the smoothing factor can now be seen: it has rendered the integration over  $t$  here relatively harmless in view of the  $(1+|t|)^{-2}$  factor. When  $c_k \equiv 1$  then  $K(s, \chi)$  can be replaced by  $L(s, \chi)$  in the above. The information needed to obtain a satisfactory bound for (8) is as follows:

- (i) A good zero-free region for  $L(s, \chi)$ . This is given by (5).
- (ii) A mean-value estimate. This is given by

$$\sum_{\chi \bmod q} \int_{-T}^T |A(s, \chi)|^2 dt \leq (qT + M) \sum_{M \leq m < 2M} m^{-2\sigma} |a_m|^2$$

which follows from [17, Theorem 6.4].

- (iii) A fourth power moment for  $L(\frac{1}{2} + it, \chi)$ . This is given by [17, Theorem 10.1] which states that

$$\sum_{\chi} \int_{-T}^T |L(s, \chi)|^4 dt \ll \phi(q) T (\log T)^4,$$

where here the summation is over primitive characters only.

- (iv) A large values estimate for Dirichlet polynomials. Such results follow from Huxley's adaptation of the Halasz method (see [13, Theorem 1], for example). The form given by (3.4) in [3] is most suitable for the present purpose. Let  $\mathcal{S}$  be a set of ordered pairs  $(t, \chi)$  with  $t \in [-T, T]$ , and  $\chi$  a character (mod  $q$ ). Suppose that  $(t_1, \chi_1), (t_2, \chi_2) \in \mathcal{S} \Rightarrow |t_1 - t_2| \geq 1$  and/or  $\chi_1 \neq \chi_2$ . If

$$|A(s, \chi)| \geq V \quad \text{for } (t, \chi) \in \mathcal{S},$$

then (3.4) in [13] states that

$$|\mathcal{S}| \ll (\log x)^2 \left( \frac{GF}{V^2} + \frac{G^3 F q T}{V^6} \right),$$

where

$$G = \sum_{M \leq m < 2M} \frac{|a_m|^2}{m}.$$

The main application combining (i), (ii) and (iv) is given by [3, Theorem 4]. This may be stated as follows.

**THEOREM.** *Suppose that  $MNK \ll x, q = x^{1-\theta}$  with  $\frac{1}{2} + \epsilon < \theta < \frac{7}{12}$ . Let  $M = x^\alpha, N = x^\beta$  with*

$$\begin{aligned} |\alpha - \beta| &< 2\theta - 1 - \epsilon, \\ 1 - (\alpha + \beta) &< \gamma(\theta) - \epsilon, \end{aligned}$$

where

$$\gamma(\theta) = \min(4\theta - 2, (20\theta - 9)/11, (72\theta - 37)/11).$$

In addition, suppose that

$$\frac{1}{1 + |t|} \left| \sum_{K \leq k < 2K} \chi(k) c_k k^{-s} \right| \ll K^{\frac{1}{2}} (\log x)^{-A} \quad (9)$$

for any  $A > 0$ . Then (8) holds.

In [3] the condition  $qT = x^\theta$  was needed, but we can drop the  $T$  factor here in view of our factor  $(1 + |t|^2)^{-1}$  in (8). Similarly we have been able to include the factor  $(1 + |t|)^{-1}$  in (9), which ensures that only small values of  $|t|$  have any significance. The reader should be able to verify that we now have all the arithmetical information analogous to that used in [11] and so obtain the result for  $q < x^{0.47}$ . The result of [16, Chapter 4] is obtained by more careful numerical analysis of the multiple integrals occurring in the method and allows us to relax the condition to  $q < x^{0.472}$ .  $\square$

#### 4. The main construction theorem

Here we combine sections 3 and 4 of [1] in such a way that we can appeal to Theorem 2. Our main result is then as follows; in the final section we sketch the deduction of Theorem 1.

**THEOREM 3.** *Let  $\epsilon > 0$ , and suppose  $y > Y(\epsilon)$ . Put*

$$\delta = \frac{\epsilon\theta}{4 \times 0.472}, \quad x = \exp(y^{1+\delta}), \quad \theta = (0.2961)^{-1}.$$

*Then there exists a positive integer  $k < x^{0.528}$  and a set of square-free numbers  $\mathcal{B}$  such that:*

- (i)  $\mathcal{B} \subset [x^{0.4}, x^{0.472}]$ ;
- (ii)  $|\mathcal{B}| > x^{\beta-\epsilon}$  with  $\beta = 0.472 \times (1 - 0.2961)$ ;
- (iii)  $dk + 1$  is prime for every  $d \in \mathcal{B}$ ;
- (iv) if  $p|d \in \mathcal{B}$  then

$$\frac{1}{2}y^\theta < p < y^\theta, \quad p \nmid k, \quad P(p-1) < y.$$

*Proof.* Rather than repeat “for all sufficiently large  $y$ ” throughout the proof, we henceforth take this for granted at each stage. Let  $f = x^{0.472}$ ,  $g = x/f$ . From [2] there is a constant  $\omega$  such that there are

$$> \frac{y^\theta}{(\log y)^\omega}$$

primes  $p$  satisfying

$$\frac{1}{2}y^\theta < p < y^\theta, \quad P(p-1) < y.$$

Let this set be  $\mathcal{A}'$ .

Let  $W = (\frac{2}{5} \log x)^{\frac{3}{4}}$ . From [5, page 93], for example, there is an absolute constant  $\eta > 0$  such that there is at most one primitive character  $\chi$  to modulus  $d < V = \exp(\eta(\log x)^{\frac{3}{4}})$ , whose L-function has a zero  $\rho$  with

$$|\operatorname{Im} \rho| \leq V, \quad \operatorname{Re} \rho > 1 - \frac{1}{W}.$$

Of course, such a zero, if it existed, would be real and a notorious Siegel zero. If such a modulus  $q$  exists and is divisible only by primes in  $\mathcal{A}'$  we remove the smallest such prime from  $\mathcal{A}'$  to get a new set  $\mathcal{A}$ . Otherwise we put  $\mathcal{A} = \mathcal{A}'$ . Let  $\mathcal{A} = \{p_1, \dots, p_r\}$ , and put

$$\begin{aligned} \mathcal{B}_0 &= \left\{ q = \prod_{j=1}^r p_j^{e_j} : e_j \in \{0, 1\}, \sum_{j=1}^r e_j \leq u \right\}, \\ \mathcal{B}_1 &= \left\{ q = \prod_{j=1}^r p_j^{e_j} : e_j \in \{0, 1\}, \sum_{j=1}^r e_j = u \right\}, \end{aligned}$$

where

$$u = \left[ \frac{\log f}{\theta \log y} \right],$$

with  $[\ ]$  denoting integer part. Then  $\mathcal{B}_1 \subset (f2^{-u}, f) \subset (x^{0.4}, f)$ . We shall choose  $\mathcal{B}$  as a suitable subset of  $\mathcal{B}_1$ . First we must remove all those  $q$  for which (5) fails. We have already shown (by removing at most one prime from  $\mathcal{A}'$  to obtain  $\mathcal{A}$ ) that (5) cannot fail if  $d \leq V$  and  $q \geq x^{0.4}$ .

Write  $N(\sigma, V, \chi)$  for the number of zeros of  $L(s, \chi)$  with  $|\operatorname{Im} s| \leq V$ ,  $\operatorname{Re} s \geq \sigma$ . Here  $\chi$  is assumed to be primitive. Various authors have obtained bounds of the form

$$\sum_{q \leq Q} \sum_{\chi \bmod q}^* N(\sigma, V, \chi) \ll (Q^2 V)^{A(1-\sigma)} \log^B(QV),$$

where  $*$  denotes summation over primitive characters only. For example, see [7] (in that paper  $B = 0$ ). It follows that, with

$$\sigma = 1 - \frac{1}{W}, \quad Q = f,$$

we have  $N(\sigma, V, \chi) = 0$  for all primitive characters to all moduli  $d > V$  with at most

$$\exp\left(D(\log x)^{\frac{1}{4}}\right)$$

exceptions up to  $f$ . Here  $D$  is an absolute constant.

Suppose that  $d$  is such an exceptional modulus and  $d \in \mathcal{B}_0$  (if  $d \notin \mathcal{B}_0$  then no  $q \in \mathcal{B}_1$  is divisible by  $d$ ). We remove all the multiples of  $d$  from  $\mathcal{B}_1$ . We have

$$|\mathcal{B}_1| = {}^r C_u.$$

If  $d$  has  $h$  prime factors then we have removed  ${}^{r-h}C_{u-h}$  members of  $\mathcal{B}_1$ . We have

$$\begin{aligned} \frac{{}^rC_u}{{}^{r-h}C_{u-h}} &= \frac{r!}{(r-h)!} \cdot \frac{(u-h)!}{u!} > \left(\frac{r}{2u}\right)^h \\ &> \left(\frac{y^\theta}{3(\log y)^\omega} \frac{\theta \log y}{0.472 \log x}\right)^h > \left(\frac{y^{\theta-1-\delta}}{(\log y)^{\omega-1}}\right)^h. \end{aligned}$$

However, since  $V \leq d \leq y^{h\theta}$ , we have  $h \geq (\log V)/(\theta \log y)$ . Thus, for some positive constant  $\alpha$ ,

$$\frac{{}^rC_u}{{}^{r-h}C_{u-h}} > \exp\left(\alpha(\log x)^{\frac{3}{4}}\right).$$

It follows that the number of integers removed from  $\mathcal{B}_1$  is

$$< {}^rC_u \exp\left(D(\log x)^{\frac{1}{4}} - \alpha(\log x)^{\frac{3}{4}}\right).$$

The resulting set of integers remaining in  $\mathcal{B}_1$ , say  $\mathcal{B}_2$ , then satisfies

$$|\mathcal{B}_2| > \frac{1}{2} {}^rC_u > x^{\beta-\epsilon/2},$$

working as on page 718 of [1].

For each  $d \in \mathcal{B}_2$ , by Theorem 2, we have

$$\pi(dg; d, 1) > \frac{cgd}{\phi(d) \log x}.$$

On the other hand, the version of the Brun-Titchmarsh inequality in [18] gives

$$\pi(gd; dq, 1) < \frac{2dg}{\phi(dq) \log(g/q)} < \frac{4dg}{\phi(d)q \log x}$$

for  $q \in \mathcal{A}$ . Since

$$\sum_{q \in \mathcal{A}} \frac{1}{q} \ll \frac{1}{\log y},$$

we deduce that there are

$$> \frac{cdg}{2\phi(d) \log x}$$

primes up to  $gd$  with  $p \equiv 1 \pmod{d}$ , but  $p \not\equiv 1 \pmod{dq}$  for any  $q \in \mathcal{A}$ . For each of these primes  $p$  there is an integer  $k \leq g$  with  $(k, q) = 1$  for every  $q \in \mathcal{A}$  and  $p = 1 + dk$ . From the lower bound for  $|\mathcal{B}_2|$  we conclude that there is one value of  $k$  which works for  $> x^{\beta-\epsilon}$  values of  $d \in \mathcal{B}_2$ . We take these values of  $d$  for our set  $\mathcal{B}$  and then (i)-(iv) hold and the proof is complete.  $\square$

## 5. Deduction of Theorem 1

We shall be brief since most details are unchanged from [1]. In this section we write  $N(L)$  for the cardinality of the largest set of residues mod  $L$  (not necessarily distinct) such that the product of terms in no non-empty subset is congruent to 1 mod  $L$ .

*Proof Theorem 1.* By Korselt's criterion,  $n$  is a Carmichael number if and only if  $n$  is square-free and  $(p-1) \mid (n-1)$  for all primes  $p \mid n$ . If  $n$  is square-free we thus



require  $\mathcal{L} \mid (n-1)$  where

$$\mathcal{L} = \text{lcm}_{p \mid n}(p-1).$$

We follow [1] in constructing  $L$  with  $\mathcal{L} \mid L$  and  $L \mid (n-1)$ , which clearly suffices. We start by putting

$$L' = \text{lcm}_{d \in \mathcal{B}} d, \quad L = kL'.$$

Since  $kd+1$  is prime for all  $d \in \mathcal{B}$ , we can find  $n \equiv 1 \pmod{L'}$  by taking  $n$  as a combination of primes  $kd+1$ . Since all these primes satisfy  $p \equiv 1 \pmod{k}$  and  $(k, L') = 1$  we have  $n \equiv 1 \pmod{L}$  as required. Also,  $p-1 \mid L$  for every  $p \mid n$ . Now the number of primes required to get  $n$  is no more than  $N(L)+1$ , and by Theorem 1.1 in [1]

$$N(L) < \lambda(L') \left( 1 + \log \left( \frac{\phi(L')}{\lambda(L')} \right) \right) < \lambda(L')(1 + \log L),$$

where

$$\lambda(L') = \text{lcm}_{q \mid L'}(q-1).$$

In fact the result we need is a special case of Proposition 1.2 in [1]:

**THEOREM 4.** *Suppose that  $r > t > n = N(L)$ . Then any set of  $r$  residues mod  $L$  contains at least  ${}^r C_t / {}^r C_n$  distinct subsets of length at most  $t$  and at least  $t-n$ , the product of whose terms is  $1 \pmod{L}$ .*

We take the members of the set as the primes  $p = kd+1$  reduced mod  $L$ . Each subset from the above result will then correspond to a distinct Carmichael number. The significance of part (iv) of Theorem 3 should now be apparent. Since  $p \mid (q-1) \Rightarrow p < y$  and  $q < p^\theta$  we have

$$\lambda(L') \leq \prod_{p < y} p^\theta \leq \exp(2\theta y).$$

On the other hand,

$$\log L \leq 2y^\theta.$$

The reader can now see why it is vital that  $\log x$  grows faster than  $y$ . We can take  $r = x^{\beta-\epsilon}$  in Theorem 4 and let  $t = \exp(y^{1+\delta/2})$ . The calculation on page 719 of [1] then goes through to complete the proof.  $\square$

*Acknowledgements.* The author would like to thank the referee for his helpful comments and Professor Carl Pomerance for pointing out the work in [15].

### References

1. W.R. ALFORD, A. GRANVILLE and C. POMERANCE, 'There are infinitely many Carmichael numbers', *Annals of Math.* 140 (1994), 703-722.
2. R.C. BAKER and G. HARMAN, 'Shifted primes without large prime factors', *Acta Arithmetica* 83 (1998) 331-361.
3. R.C. BAKER, G. HARMAN and J. PINTZ, 'The exceptional set for Goldbach's problem in short intervals', *Sieve Methods, Exponential Sums and their Applications in Number Theory* (ed. G.R.H. Greaves, G. Harman and M.N. Huxley), (Cambridge University Press 1997), 1-54.

4. R. C. BAKER, G. HARMAN and J. PINTZ, 'The difference between consecutive primes, II', *Proc. London Math. Soc.* (3) 83 (2001) 532-562.
5. H. DAVENPORT, *Multiplicative Number Theory*, 2nd edn, revised by H.L. Montgomery (Springer, New York 1980).
6. J. B. FRIEDLANDER, 'Shifted primes without large prime factors', in *Number Theory and Applications* (ed R.A. Mollin) (Kluwer, NATO ASI, 1989), 393-401.
7. P. X. GALLAGHER, 'A large sieve density estimate near  $\sigma = 1$ ', *Invent. Math.* 16 (1970) 329-339.
8. A. GRANVILLE and C. POMERANCE, 'Two contradictory conjectures concerning Carmichael numbers', *Math. Comp.* 71 (2002), 883-908.
9. G. HARMAN, 'On the distribution of  $\alpha p$  modulo one', *J. London Math. Soc.* (2) 27 (1983) 9-18.
10. G. HARMAN, 'On the distribution of  $\alpha p$  modulo II', *Proc. London Math. Soc.* (3) 72 (1996) 241-260.
11. G. HARMAN, A. KUMCHEV and P.A. LEWIS, 'The distribution of prime ideals of quadratic imaginary fields', *Trans. American Math. Soc.* 356 (2004), 599-620.
12. G. HARMAN, N. WATT and K. WONG, 'A new mean-value result for Dirichlet L-functions and polynomials', *Quart. J. Math. Oxford* 55 (2004), 307-324.
13. M. N. HUXLEY, 'Large values of Dirichlet Polynomials III', *Acta Arithmetica* 26 (1975) 435-444.
14. A. KUMCHEV, 'The difference between consecutive primes in an arithmetic progression', *Quart. J. Math. Oxford* 53 (2002) 479-501.
15. H.W. LENSTRA JR AND C. POMERANCE, 'Primality testing with Gaussian periods', *to appear*.
16. P. A. LEWIS, *Finding information about Gaussian primes using analytic number theory sieve methods*, Ph.D Thesis (Cardiff 2002).
17. H. L. MONTGOMERY, *Topics in Multiplicative Number Theory*, Lecture Notes in Mathematics 227 (Springer, New York, 1971).
18. H. L. MONTGOMERY AND R. C. VAUGHAN, 'The large sieve', *Mathematika* 20 (1973), 119-134.
19. E. C. TITCHMARSH, *Theory of the Riemann Zeta-function* (second edition revised by D. R. Heath-Brown), (Clarendon Press, Oxford, 1986).
20. N. WATT, 'Kloosterman sums and a mean value result for Dirichlet polynomials', *J. Number Theory* 53 (1995) 179-210.

*Department of Mathematics,*  
*Royal Holloway, University of*  
*London,*  
*EGHAM,*  
*Surrey TW20 0EX*  
 g.harman@rhul.ac.uk