Sierpiński and Carmichael numbers

William Banks
Department of Mathematics
University of Missouri
Columbia, MO 65211, USA
bbanks@math.missouri.edu

Carrie Finch
Mathematics Department
Washington and Lee University
Lexington, VA 24450, USA
finchc@wlu.edu

Florian Luca
Centro de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58089, Morelia, Michoacán, México
fluca@matmor.unam.mx

Carl Pomerance
Department of Mathematics
Dartmouth College
Hanover, NH 03755-3551 USA
carl.pomerance@dartmouth.edu

Pantelimon Stănică
Department of Applied Mathematics
Naval Postgraduate School
Monterey, CA 93943, USA
pstanica@nps.edu

September 30, 2012

Abstract

We establish several related results on Carmichael, Sierpiński and Riesel numbers. First, we prove that almost all odd natural numbers k have the property that 2^nk+1 is not a Carmichael number for any $n \in \mathbb{N}$; this implies the existence of a set $\mathcal{K}$ of positive lower density such that for any $k \in \mathcal{K}$ the number 2^nk+1 is neither prime nor Carmichael for every $n \in \mathbb{N}$. Next, using a recent result of Matomäki, we show that there are $\gg x^{1/5}$ Carmichael numbers up to x that are also Sierpiński and Riesel. Finally, we show that if 2^nk+1 is Lehmer, then $n \leqslant 150\,\omega(k)^2 \log k$, where $\omega(k)$ is the number of distinct primes dividing k.

1 Introduction

In 1960, Sierpiński [25] showed that there are infinitely many odd natural numbers k with the property that 2^nk+1 is composite for every natural number n; such an integer k is called a *Sierpiński number* in honor of his work. Two years later, J. Selfridge (unpublished) showed that 78557 is a Sierpiński number, and this is still the smallest known example.[1]

Every currently known Sierpiński number k possesses at least one *covering set* $\mathcal{P}$, which is a finite set of prime numbers with the property that 2^nk+1 is divisible by some prime in $\mathcal{P}$ for every $n \in \mathbb{N}$. For example, Selfridge showed that 78557 is Sierpiński by proving that every number of the form $2^n{\cdot}78557+1$ is divisible by a prime in $\mathcal{P} := \{3,5,7,13,19,37,73\}$. When a covering set is used to show that a given number is Sierpiński, every natural number in a certain arithmetic progression (determined by the covering set) must also be Sierpiński; in particular, the set of Sierpiński numbers has a positive lower density.

If N is a prime number, *Fermat's little theorem* asserts that

$$a^N \equiv a \pmod N \qquad \text{for all } a \in \mathbb{Z}. \tag{1}$$

Around 1910, Carmichael [9, 10] initiated the study of composite numbers N with the same property; these are now known as *Carmichael numbers*. In 1994, Alford, Granville and Pomerance [1] proved the existence of infinitely

[1] At present, there are only six smaller numbers that *might* have the Sierpiński property: 10223, 21181, 22699, 24737, 55459, 67607; see `http://www.seventeenorbust.com` for the most up-to-date information.

many Carmichael numbers. Since prime numbers and Carmichael numbers share the property (1), it is natural to ask whether certain results for primes can also be established for Carmichael numbers; see, for example, [2, 3, 5, 14, 20, 29] and the references contained therein.

Our work in this paper originated with the question as to whether there exist Sierpiński numbers k such that $2^n k + 1$ is *not* a Carmichael number for any $n \in \mathbb{N}$. Since there are many Sierpiński numbers and only a few Carmichael numbers, it is natural to expect there are many such k. However, because the parameter n can take any positive integer value, the problem is both difficult and interesting. Later on, we dropped the condition that k be Sierpiński and began to study odd numbers k for which $2^n k + 1$ is never a Carmichael number. Our main result is the following theorem.

Theorem 1. *Almost all odd natural numbers k have the property that $2^n k+1$ is not a Carmichael number for any $n \in \mathbb{N}$.*

This is proved in §2. Our proof uses results and methods from a recent paper of Cilleruelo, Luca and Pizarro-Madariaga [11], where it is shown that the bound

$$n \leqslant 2^{2000000\,\tau(k)^2\omega(k)(\log k)^2} \tag{2}$$

holds for every Carmichael number $2^n k + 1$. Here, $\tau(k)$ is the number of positive integer divisors of k, and $\omega(k)$ is the number of distinct prime factors of k. To give some perspective on this result, let $v_2(\cdot)$ be the standard 2-adic valuation, so that $2^{-v_2(m)}m$ is the odd part of any natural number m. Theorem 1 implies that the set

$$\big\{k = 2^{-v_2(n-1)}(n-1) : n \text{ is a Carmichael number}\big\}$$

has asymptotic density zero.[2] By comparison, Erdős and Odlyzko [15] have shown that the set

$$\big\{k = 2^{-v_2(p-1)}(p-1) : p \text{ is a prime number}\big\}$$

has a positive lower density.

Since the collection of Sierpiński numbers has a positive lower density, the following corollary is an immediate consequence of Theorem 1.

[2] In [11] it is shown that 27 is the smallest number in this set.

Corollary 1. *There exists a set* $\mathcal{K} \subseteq \mathbb{N}$ *of positive lower density such that for any fixed* $k \in \mathcal{K}$*, the number* $2^n k + 1$ *is neither prime nor Carmichael for each* $n \in \mathbb{N}$*.*

Riesel numbers have a similar definition to that of Sierpiński numbers. An odd natural number k is called a *Riesel number* if $2^n k - 1$ is composite for all $n \in \mathbb{N}$. Such numbers were first investigated in 1956 by Riesel [24]. At present, the smallest known example is 509203.[3] It is known that there are infinitely many natural numbers that are both Sierpiński and Riesel. Using a recent result of Matomäki [20] and Wright [29] coupled with an extensive computer search, we prove the following result in §3.

Theorem 2. *Infinitely many natural numbers are simultaneously Sierpiński, Riesel, and Carmichael. In fact, the number of them up to* x *is* $\gg x^{1/5}$ *for all sufficiently large* x*.*

Let $\varphi(\cdot)$ be the *Euler function*, which is defined by $\varphi(n) := n \prod_{p \mid n}(1-p^{-1})$ for all $n \in \mathbb{N}$; in particular, one has $\varphi(p) = p - 1$ for every prime p. In 1932, Lehmer [19] asked whether there are any composite numbers n such that $\varphi(n) \mid n - 1$, and the answer to this question is still unknown. We say that n is a *Lehmer number* if n is composite and $\varphi(n) \mid n - 1$. It is easy to see that every Lehmer number is Carmichael, but there are infinitely many Carmichael numbers which are not Lehmer (see [4]). We prove the following result in §4.

Theorem 3. *Let* k *be an odd natural number. If* $2^n k + 1$ *is Lehmer, then* $n \leqslant 150\,\omega(k)^2 \log k$*. If* $2^n k - 1$ *is Lehmer, then* $n = 1$*.*

Throughout the paper, we use $\log_k x$ to denote the k-th iterate of the function $\log x := \max\{\ln x, 1\}$, where $\ln x$ is the natural logarithm. We use the notations O, o, $\ll$, $\gg$ with their customary meanings. Any constant or function implied by one of these symbols is absolute unless otherwise indicated.

Acknowledgments. The authors thank Jan-Hendrik Evertse for helpful advice and for providing some references. They also thank Pedro Berrizbeitia for an enlightening conversation. The third-named author was supported in

[3] As of this writing, there are 55 candidates smaller that 509203 to consider; see `http://www.prothsearch.net/rieselprob.html` for the most recent information.

part by Project PAPIIT 104512 and a Marcos Moshinsky fellowship. The fourth-named author would like to acknowledge support from NSF grant DMS-1001180.

2 Proof of Theorem 1

2.1 Preliminary estimates

Let x be a large real parameter, and put

$$\mathcal{C}(x) := \big\{\text{odd } k \in (x/2, x] : 2^n k + 1 \text{ is Carmichael for some } n\big\}.$$

If $\mathcal{S}(x) \subseteq \mathcal{C}(x)$ for all large x, we say that $\mathcal{S}(x)$ is *negligible* if $|\mathcal{S}(x)| = o(x)$ as $x \to \infty$. Below, we construct a sequence $\mathcal{C}_1(x), \mathcal{C}_2(x), \ldots$ of negligible subsets of $\mathcal{C}(x)$, and for each $j \geqslant 1$ we denote

$$\mathcal{C}_j^*(x) := \mathcal{C}(x) \setminus \bigcup_{i=1}^{j} \mathcal{C}_i(x).$$

Theorem 1 is the statement that $\mathcal{C}(x)$ is itself negligible; thus, we need to show that $\mathcal{C}_j^*(x)$ is negligible for some j.

Let $\Omega(n)$ be the number of prime factors of n, counted with multiplicity, and put

$$\mathcal{N}_1(x) := \big\{k \leqslant x : \Omega(k) > 1.01 \log_2 x\big\}.$$

Since $\log_2 x$ is the normal order of $\Omega(n)$ over numbers $n \leqslant x$, it follows that

$$|\mathcal{N}_1(x)| = o(x) \qquad (x \to \infty). \tag{3}$$

In fact, using the Turán-Kubilius inequality (see [27]) one sees that $|\mathcal{N}_1(x)| \ll x/\log_2 x$, and stronger bounds can be deduced from results in the literature (although they are not needed here). Using (3) it follows that

$$\mathcal{C}_1(x) := \mathcal{C}(x) \cap \mathcal{N}_1(x)$$

is negligible.

Next, let $\Omega(z; n)$ denote the number of prime factors $p \le z$ of n, counted with multiplicity. Set

$$\mathcal{N}_2(x) := \big\{k \leqslant x : \Omega(z_1; k) > 2 \log_3 x\big\} \qquad \text{with} \quad z_1 := (\log x)^{10}.$$

Since the normal order of $\Omega(z_1; n)$ over numbers $n \leqslant x$ is $\log_2 z_1 \sim \log_3 x$, it follows that $|\mathcal{N}_2(x)| = o(x)$ as $x \to \infty$; therefore,

$$\mathcal{C}_2(x) := \mathcal{C}(x) \cap \mathcal{N}_2(x)$$

is negligible.

In what follows, we denote

$$y_{\rm L} := x^{1/2-10\varepsilon} \qquad \text{and} \qquad y_{\rm U} := x^{1/2+10\varepsilon},$$

where

$$\varepsilon = \varepsilon(x) := \frac{1}{\log_2 x}.$$

According to Tenenbaum [26, Théorème 1] (see also Ford [17, Theorem 1]) there are precisely $x/(\log_2 x)^{\delta+o(1)}$ numbers $k \leqslant x$ that have a divisor $d \in [y_{\rm L}, y_{\rm U}]$, where $\delta := 1 - (1 + \ln\ln 2)/\ln 2$; in particular, the set

$$\mathcal{N}_3(x) := \big\{k \leqslant x : k \text{ has a divisor } d \in [y_{\rm L}, y_{\rm U}]\big\}$$

is such that $|\mathcal{N}_3(x)| = o(x)$ as $x \to \infty$; therefore,

$$\mathcal{C}_3(x) := \mathcal{C}(x) \cap \mathcal{N}_3(x)$$

is negligible.

For each $k \in \mathcal{C}(x)$, let $n_0(k)$ be the least $n \in \mathbb{N}$ for which $2^n k + 1$ is a Carmichael number. For any real $X \geqslant 1$ let

$$\mathcal{F}(X) := \big\{k \in \mathcal{C}(x) : n_0(k) \leqslant X\big\},$$

and for any subset $\mathcal{Q} \subseteq \mathbb{N}$, let $\mathcal{F}(\mathcal{Q}; X)$ be the set of $k \in \mathcal{F}(X)$ for which there exists $n \leqslant X$ with the property that $2^n k + 1$ is a Carmichael number divisible by some number $q \in \mathcal{Q}$.

Lemma 1. *If X and $\mathcal{Q}$ are both defined in terms of x, and one has*

$$X \sum_{q \in \mathcal{Q}} q^{-1} = o(1) \qquad \textit{and} \qquad X|\mathcal{Q}| = o(x) \qquad (x \to \infty),$$

then $\big|\mathcal{F}(\mathcal{Q}; X)\big| = o(x)$ as $x \to \infty$.

Proof. For fixed $n \leqslant X$ and $q \in \mathcal{Q}$, if $2^n k + 1$ is a Carmichael number that is divisible by q, then k lies in the arithmetic progression $-2^{-n} \bmod q$; thus, the number of such $k \leqslant x$ cannot exceed $x/q + 1$. Summing over all $n \leqslant X$ and $q \in \mathcal{Q}$ we derive that

$$\big|\mathcal{F}(\mathcal{Q}; X)\big| \leqslant \sum_{\substack{n \leqslant X \\ q \in \mathcal{Q}}} (x/q + 1) \leqslant xX \sum_{q \in \mathcal{Q}} q^{-1} + X|\mathcal{Q}| = o(x) \qquad (x \to \infty),$$

as required. □

2.2 Small values of $n_0(k)$

Consider the set

$$\mathcal{C}_4(x) := \mathcal{F}(X_1), \qquad \text{where} \quad X_1 := \frac{\log x}{\log_2 x}.$$

According to Pomerance [22] there are $\ll t/L(t)$ Carmichael numbers that do not exceed t, where

$$L(t) := \exp\left(\frac{\log t \, \log_3 t}{\log_2 t}\right).$$

Since the function $f(k) := 2^{n_0(k)} k + 1$ is one-to-one and maps $\mathcal{C}_4(x)$ into the set of Carmichael numbers not exceeding $2^{X_1} x + 1$, we have

$$|\mathcal{C}_4(x)| \ll \frac{2^{X_1} x}{L(2^{X_1} x)} = \frac{x}{L(x)^{1+o(1)}} = o(x) \qquad (x \to \infty).$$

In other words, $\mathcal{C}_4(x)$ is negligible.

2.3 Medium values of $n_0(k)$

Our aim in this subsection is to show that

$$\mathcal{S}(x) := \mathcal{F}(X_2) \setminus \mathcal{F}(X_1) \qquad \text{with} \quad X_2 := \exp\left(\frac{\log x}{\log_2 x}\right)$$

is negligible. To do this, we define five more negligible sets $\mathcal{C}_5(x), \ldots, \mathcal{C}_9(x)$ and show that $\mathcal{S}(x)$ is contained in $\bigcup_{i=1}^{9} \mathcal{C}_i(x)$. We denote

$$\mathcal{S}_j^*(x) := \mathcal{S}(x) \setminus \bigcup_{i=1}^{j} \mathcal{C}_i(x) \qquad (1 \leqslant j \leqslant 9).$$

As before, we put

$$z_1 := (\log x)^{10}, \qquad y_{\rm L} := x^{1/2-10\varepsilon}, \qquad y_{\rm U} := x^{1/2+10\varepsilon}, \qquad \varepsilon := \frac{1}{\log_2 x}.$$

Note that $X_2 = x^\varepsilon$ with this notation.

Let $N := 2^n k + 1$ be a Carmichael number with $k \in \mathcal{S}_4^*(x)$ and $n \leqslant X_2$. For any prime p dividing N we have $p - 1 \mid N - 1 = 2^n k$ (the well–known Korselt's criterion); thus, $p = 2^m d + 1$ for some $m \leqslant n$ and some divisor $d \mid k$. Note that $d \notin [y_{\rm L}, y_{\rm U}]$ since $k \notin \mathcal{C}_3(x)$.

Suppose that $d > y_{\rm U}$. Writing $k = dd_1$ we see that $d_1 \leqslant x/d < x/y_{\rm U} = y_{\rm L}$. Furthermore, $2^{n-m} d_1 = (N-1)/(p-1) \equiv 1 \pmod p$; that is, $p \mid 2^{n-m} d_1 - 1$. Note that $2^{n-m} d_1 - 1 = (N-p)/(p-1)$ is nonzero since N is Carmichael, hence composite.

Now let $\mathcal{P}$ be the set of primes of the form $2^m d + 1$ with $m \leqslant X_2$ and $d \in [y_{\rm U}, x]$, and let $\mathcal{P}_1$ be the subset of $\mathcal{P}$ consisting of those primes p that divide at least one Carmichael number $N = 2^n k + 1$ with $k \in \mathcal{S}_4^*(x)$ and $n \leqslant X_2$. In view of the above discussion we have

$$\prod_{p \in \mathcal{P}_1} p \;\Bigg|\; \prod_{\substack{0 \leqslant \ell \leqslant X_2 \\ d_1 \leqslant y_{\rm L} \\ (\ell, d_1) \neq (0,1)}} (2^\ell d_1 - 1) \leqslant \prod_{\substack{0 \leqslant \ell \leqslant X_2 \\ d_1 \leqslant y_{\rm L}}} e^{X_2} \leqslant \exp(2X_2^2 y_{\rm L}).$$

Here, we have used the fact that $2^\ell d_1 - 1 \leqslant 2^{X_2} y_{\rm L} \leqslant e^{X_2}$ holds for $x > x_0$. Since $p \geqslant y_{\rm U} \geqslant x^{1/2}$ for all $p \in \mathcal{P}$, it follows that

$$|\mathcal{P}_1| \leqslant \frac{\log\left(\prod_{p \in \mathcal{P}_1} p\right)}{\log(x^{1/2})} \leqslant \frac{4X_2^2 y_{\rm L}}{\log x} = \frac{4x^{1/2-8\varepsilon}}{\log x}$$

for $x > x_0$; in particular, $X_2 |\mathcal{P}_1| = o(x)$ as $x \to \infty$. Using this inequality for $|\mathcal{P}_1|$ we also have

$$X_2 \sum_{p \in \mathcal{P}_1} p^{-1} \leqslant \frac{X_2 |\mathcal{P}_1|}{y_{\rm U}} \leqslant \frac{4x^{-17\varepsilon}}{\log x} = o(1) \qquad (x \to \infty).$$

Applying Lemma 1 we see that the set

$$\mathcal{C}_5(x) := \mathcal{S}_4^*(x) \cap \mathcal{F}(\mathcal{P}_1; X_2) = \mathcal{C}_4^*(x) \cap \mathcal{F}(\mathcal{P}_1; X_2)$$

is negligible.

Similarly, let $\mathcal{P}_2$ be the set of primes of the form $2^m d+1$ with $m \geqslant \log x$ and $d \leqslant y_{\rm L}$. Clearly, for $x > x_0$ we have the bound

$$|\mathcal{P}_2| \leqslant \big|\big\{(m,d) : 1 \leqslant m \leqslant X_2,\ d \leqslant y_{\rm L}\big\}\big| \leqslant X_2 y_{\rm L} = x^{1/2-9\varepsilon}. \tag{4}$$

Therefore, $X_2|\mathcal{P}_2| = o(x)$ as $x \to \infty$. Moreover,

$$X_2 \sum_{p\in\mathcal{P}_2} p^{-1} \leqslant \frac{X_2|\mathcal{P}_2|}{2^{\log x}} \leqslant x^{1/2-\log 2-8\varepsilon} = o(1) \qquad (x \to \infty).$$

Applying Lemma 1 we see that the set

$$\mathcal{C}_6(x) := \mathcal{S}_5^*(x) \cap \mathcal{F}(\mathcal{P}_2; X_2) = \mathcal{C}_5^*(x) \cap \mathcal{F}(\mathcal{P}_2; X_2)$$

is negligible.

We now take a moment to observe that for every $k \in \mathcal{S}_6^*(x)$ one has

$$n_0(k) \leqslant X_3 \qquad \text{with} \quad X_3 := (\log x)^3.$$

Indeed, let $2^n k+1$ be a Carmichael number such that $n \leqslant X_2$. If $p \mid 2^n k+1$, then $p = 2^m d+1$ with $m \leqslant \log x$, $d \leqslant y_{\rm L}$ and $d \mid k$. Taking into account that $d \leqslant y_{\rm L} \leqslant x^{1/2} \leqslant 2^{\log x} - 1$ for $x > x_0$, it follows that $2^m d+1 \leqslant 2^{2\log x}$, and so

$$2^n \leqslant 2^n k+1 \leqslant \prod_{\substack{m\leqslant \log x\\ d\leqslant y_{\rm L},\ d\mid k}} (2^m d+1) \leqslant 2^{2(\log x)^2\tau(k)}.$$

Since $k \notin \mathcal{N}_1(x)$ we have

$$\tau(k) \leqslant 2^{\Omega(k)} \leqslant 2^{1.01\log_2 x} \leqslant (\log x)^{0.8}, \tag{5}$$

and therefore,

$$n \leqslant 2(\log x)^{2.8} \leqslant X_3 \qquad (x > x_0).$$

Let $\mathcal{P}_3$ be the set of primes of the form $2^m d+1$ with $m \geqslant M$ and $d \leqslant y_{\rm L}$, where

$$M := 10\log_2 x.$$

The estimation in (4) shows that $|\mathcal{P}_3| \leqslant x^{1/2-9\varepsilon}$; thus $X_3|\mathcal{P}_3| = o(x)$ as $x \to \infty$. Also,

$$X_3 \sum_{p\in\mathcal{P}_3} p^{-1} \leqslant X_3\bigg(\sum_{m\geqslant M} 2^{-m}\bigg)\bigg(\sum_{d\leqslant y_{\rm L}} d^{-1}\bigg) \ll (\log x)^{4-10\log 2} = o(1)$$

as $x \to \infty$. By Lemma 1 it follows that the set

$$\mathcal{C}_7(x) := \mathcal{S}_6^*(x) \cap \mathcal{F}(\mathcal{P}_3; X_3) = \mathcal{C}_6^*(x) \cap \mathcal{F}(\mathcal{P}_3; X_3)$$

is negligible.

Next, let $\mathcal{Q}_1$ be the collection of almost primes of the form $q = p_1 p_2$, where $p_1 = 2^{m_1} d + 1$, $p_2 = 2^{m_2} d + 1$, $m_1 < m_2 \leqslant M$, and $d > z_1$. Here, $M := 10 \log_2 x$ and $z_1 := (\log x)^{10}$ as before. Clearly, the bound

$$|\mathcal{Q}_1| \leqslant \left|\left\{(m_1, m_2, d) : m_1, m_2 \leqslant M,\ d \leqslant y_{\rm L}\right\}\right| \leqslant M^2 y_{\rm L} \leqslant x^{1/2-9\varepsilon}$$

holds if $x > x_0$, and thus $X_3 |\mathcal{Q}_1| = o(x)$ as $x \to \infty$. Also,

$$X_3 \sum_{q \in \mathcal{Q}_1} q^{-1} \leqslant X_3 \Bigg(\sum_{m \geqslant 1} 2^{-m}\Bigg)^2 \Bigg(\sum_{d > z_1} d^{-2}\Bigg) \ll \frac{X_3}{z_1} = (\log x)^{-7} = o(1)$$

as $x \to \infty$. Applying Lemma 1 again, we see that

$$\mathcal{C}_8(x) := \mathcal{S}_7^*(x) \cap \mathcal{F}(\mathcal{Q}_1; X_3) = \mathcal{C}_7^*(x) \cap \mathcal{F}(\mathcal{Q}_1; X_3)$$

is negligible.

Similarly, let $\mathcal{Q}_2$ be the collection of almost primes of the form $q = p_1 p_2$, where $p_1 = 2^{m_1} d_1 + 1$, $p_2 = 2^{m_2} d_2 + 1$, $m_1 < m_2 \leqslant M$, $d_1, d_2 \leqslant y_{\rm L}$, and $\gcd(d_1, d_2)$ is divisible by some prime $r > z_1$. We have

$$|\mathcal{Q}_2| \leqslant \left|\left\{(m_1, m_2, d_1, d_2) : m_1, m_2 \leqslant M,\ d_1, d_2 \leqslant y_{\rm L}\right\}\right| \leqslant M^2 y_{\rm L}^2 \leqslant x^{1-19\varepsilon}$$

if $x > x_0$, hence $X_3 |\mathcal{Q}_2| = o(x)$ as $x \to \infty$. Furthermore,

$$\begin{aligned}\sum_{q \in \mathcal{Q}_2} q^{-1} &\leqslant \Bigg(\sum_{m \geqslant 1} 2^{-m}\Bigg)^2 \Bigg(\sum_{\substack{d_1 = ru \leqslant y_{\rm L} \\ d_2 = rv \leqslant y_{\rm L} \\ r > z_1}} (d_1 d_2)^{-1}\Bigg) \\ &\ll \Bigg(\sum_{r > z_1} r^{-2}\Bigg) \Bigg(\sum_{u \leqslant y_{\rm L}} u^{-1}\Bigg)^2 \ll (\log x)^{-8},\end{aligned}$$

and therefore

$$X_3 \sum_{q \in \mathcal{Q}_2} q^{-1} \ll (\log x)^{-5} = o(1) \qquad (x \to \infty).$$

By Lemma 1 the set

$$\mathcal{C}_9(x) := \mathcal{S}_8^*(x) \cap \mathcal{F}(\mathcal{Q}_2; X_3) = \mathcal{C}_8^*(x) \cap \mathcal{F}(\mathcal{Q}_2; X_3)$$

is negligible.

To conclude this subsection, we now show that $\mathcal{S}_9^*(x) = \varnothing$; this implies that $\mathcal{S}(x)$ is contained in $\mathcal{C}_1(x) \cup \cdots \cup \mathcal{C}_9(x)$ as claimed.

Suppose on the contrary that $\mathcal{S}_9^*(x) \neq \varnothing$. For each $k \in \mathcal{S}_9^*(x)$ there exists $n \in (X_1, X_3]$ such that $2^n k + 1$ is Carmichael; let

$$2^n k + 1 = \prod_{j=1}^{\ell} (2^{m_j} d_j + 1) \tag{6}$$

be its factorization into (distinct) primes. Grouping the primes on the right side of (6) according to the size of d_j, we set

$$A := \prod_{\substack{1 \leqslant j \leqslant \ell \\ d_j \leqslant z_1}} (2^{m_j} d_j + 1) \qquad \text{and} \qquad B := \frac{2^n k + 1}{A}.$$

For every prime $p_j := 2^{m_j} d_j + 1$ dividing A we have $m_j < M$ since $k \notin \mathcal{C}_7(x)$; therefore,

$$p_j \leqslant 2^{M+1} z_1 = 2^{10 \log_2 x + 1 + (10/\log 2) \log_2 x} \leqslant 2^{30 \log_2 x} = 2^{3M}.$$

Taking into account the bound (5), we see that

$$A \leqslant \prod_{\substack{d \mid k \\ m < M}} 2^{3M} \leqslant 2^{3M^2 \tau(k)} \leqslant 2^{300 (\log_2 x)^2 (\log x)^{0.8}} \leqslant 2^{(\log x)^{0.9}} \qquad (x > x_0). \tag{7}$$

On the other hand, every prime $p_j := 2^{m_j} d_j + 1$ dividing B has $d_j > z_1$. Since each $m_j < M$ and $k \notin \mathcal{C}_8(x)$, it follows that the divisors d_j are different for distinct primes p_j dividing B. For any such divisor d_j, factor $d_j = d_j^- d_j^+$, where d_j^- [resp. d_j^+] is the largest divisor of d that is composed solely of primes $\leqslant z_1$ [resp. $> z_1$]. The numbers $\{d_j^+\}$ are coprime in pairs since $k \notin \mathcal{C}_9(x)$; consequently,

$$\prod_{p_j \mid B} d_j^+ \leqslant k$$

as the product on the left side is a divisor of k. As for the numbers $\{d_j^-\}$, we note that

$$d_j^- \leqslant z_1^{\Omega(z_1;k)} \leqslant (\log x)^{20\log_3 x} \leqslant 2^{(\log_2 x)^2} \qquad (x > x_0),$$

where we have used the fact that $k \notin \mathcal{N}_2(x)$ for the second inequality. Putting everything together, we derive the bound

$$B \leqslant \prod_{p_j \mid B} 2^{M+1} d_j^- d_j^+ \leqslant (2^{10\log_2 x + 1 + (\log_2 x)^2})^{\tau(k)} \prod_{p_j \mid B} d_j^+ \leqslant 2^{(\log x)^{0.9}} k \qquad (8)$$

for all $x > x_0$. Combining (6), (7) and (8) it follows that

$$2^n k + 1 = AB \leqslant 2^{2(\log x)^{0.9}} k,$$

and therefore, $n \leqslant 2(\log x)^{0.9}$. However, since $n > X_1 = (\log x)/\log_2 x$ this is impossible for large x. The contradiction implies that $\mathcal{S}_9^*(x) = \varnothing$ as claimed.

2.4 Large values of $n_0(k)$

Recall that a number k is said to be *powerful* if $p^2 \mid k$ for every prime p dividing k. We denote

$$\mathcal{C}_{10}(x) := \big\{k \leqslant x : k \text{ is powerful}\big\}.$$

By the well known bound $|\mathcal{C}_{10}(x)| \ll x^{1/2}$, the set $\mathcal{C}_{10}(x)$ is negligible.

From now on, fix $k \in \mathcal{C}_{10}^*(x)$, and let $n > X_2 := \exp((\log x)/\log_2 x)$ be such that $2^n k + 1$ is a Carmichael number. Also, let $p = 2^m d + 1$ be a fixed prime factor of $2^n k + 1$. For convenience, we denote

$$N_1 := \left\lfloor \sqrt{\frac{n}{\log x}} \right\rfloor \qquad \text{and} \qquad N_2 := \frac{n}{N_1}.$$

Since numbers of the form $um + vn$ with $(u, v) \in [0, N_1]^2$ all lie in the interval $[0, 2nN_1]$, and there are $(N_1+1)^2$ such pairs (u, v), by the pigeonhole principle there exist $(u_1, v_1) \neq (u_2, v_2)$ such that

$$\big|(u_1 m + v_1 n) - (u_2 m + v_2 n)\big| \leqslant \frac{2N_1 n}{(N_1+1)^2 - 1} \leqslant \frac{2n}{N_1} = 2N_2.$$

Put $u := u_1 - u_2$ and $v := v_1 - v_2$. Then

$$(u,v) \neq (0,0), \qquad \max\{|u|,|v|\} \leqslant N_1, \qquad |um+vn| \leqslant 2N_2. \tag{9}$$

Replacing u, v with $u/d, v/d$, where d is either $\gcd(u,v)$ or $-\gcd(u,v)$, we can further assume that

$$\gcd(u,v) = 1 \qquad \text{and} \qquad u \geqslant 0. \tag{10}$$

From the congruences

$$2^m d \equiv -1 \pmod p \qquad \text{and} \qquad 2^n k \equiv -1 \pmod p \tag{11}$$

we derive that

$$2^{um+vn} d^u k^v \equiv (-1)^{u+v} \pmod p.$$

Therefore, p divides the numerator of the rational number

$$G := 2^{um+vn} d^u k^v - (-1)^{u+v}.$$

We claim that $G \neq 0$. Indeed, suppose on the contrary that $G = 0$. Since k and d are both odd, it follows that $um + vn = 0$ and $d^u k^v = 1$. If $u = 0$ or $v = 0$, the first equation implies that $(u,v) = (0,0)$, which is not allowed; hence $uv \neq 0$, and by (10) we have $u > 0$. Since u and v are coprime, the equality $d^u = k^{-v}$ implies that $k = k_1^u$ for some $k_1 > 1$. As $k \notin \mathcal{C}_{10}(x)$, it follows that $u = 1$. Then, as $d \mid k$ and $d = k^{-v}$, we also have $v = -1$, $d = k$, and $0 = um + vn = m - n$, so $m = n$. But this shows that $2^n k + 1 = p$, which is not possible since $2^n k + 1$ is a Carmichael number. This contradiction establishes our claim that $G \neq 0$.

Since p divides the numerator of G, using (9) we derive the bound

$$p \leqslant 2^{|um+vn|} d^{|u|} k^{|v|} + 1 \leqslant 2^{2N_2+1} x^{2N_1} = 2^{(2+2/\log 2)N_2+1}, \tag{12}$$

which is used below and in §2.5. We also need the following:

Lemma 2. *Let*

$$\Delta_1 := \frac{\sqrt{2}(\log_2 x)^{3/2}}{(\log n)^{1/4}}.$$

For $x > x_0$, the Carmichael number $2^n k + 1$ has no more than $n^{1/3}$ prime divisors $p = 2^m d + 1$ with $m > \Delta_1 N_2$.

Proof. With the minor modifications outlined here, this result is essentially contained in [11, Lemma 7]. The underlying argument is fairly standard (see, for example, [6, 7, 12, 13, 18]), although it relies on a quantitative version of the *Subspace Theorem* due to Evertse [16], a bound of Pontreau [23] on the number of solutions to certain *S-unit equations*, and Baker's bound on *linear forms in logarithms* (see [21] or [8, Theorem 5]).

Let $p = 2^m d + 1$ be a prime divisor of $2^n k + 1$ with $m > \Delta_1 N_2$. Using the Euclidean algorithm, we write

$$n = mq + r \qquad \text{with} \quad 0 \leqslant r < m \leqslant 5N_2, \tag{13}$$

where the last inequality is a consequence of (12). Note that

$$q \leqslant \frac{n}{m} \leqslant \frac{n}{\Delta_1 N_2} = \Delta_1^{-1} N_1. \tag{14}$$

From (11) we obtain the congruences

$$2^{mq} d^q \equiv (-1)^q \pmod p \qquad \text{and} \qquad 2^{mq+r} k \equiv -1 \pmod p,$$

hence p divides

$$G := d^q + (-1)^q 2^r k.$$

We claim that $G \neq 0$. Indeed, suppose on the contrary that $G = 0$. Then $r = 0$ (since d is odd), q is odd, and $k = d^q$. As $k \notin \mathcal{C}_{10}(x)$, $q = 1$. But this implies that $d = k$ and $n = mq + r = m$, hence $2^n k + 1 = p$, which is impossible since $2^n k + 1$ is a Carmichael number. This contradiction establishes our claim that $G \neq 0$.

Since p divides G, using (13) and (14) we derive the bound

$$\begin{aligned} p \leqslant |G| \leqslant 2^r d^q k \leqslant 2^r x^{q+1} &\leqslant 2^{r + (q+1)(\log x)/\log 2} \\ &\leqslant 2^{5N_2 + (\Delta_1^{-1} N_1 + 1)(\log x)/\log 2} \leqslant 2^{2\Delta_1^{-1} N_2} \qquad (x > x_0). \end{aligned} \tag{15}$$

We also have the lower bound

$$p - 1 = 2^m d \geqslant 2^m > 2^{\Delta_1 N_2}. \tag{16}$$

Put

$$U := 2^m d, \qquad V_1 := d^q \qquad \text{and} \qquad V_2 := (-1)^q 2^r k.$$

Then, taking into account the fact that $V_1 + V_2 = G$, the inequalities (15) and (16) together imply that

$$U > |V_1 + V_2|^{\Delta_2} \qquad \text{with} \quad \Delta_2 := \tfrac{1}{2}\Delta_1^2 = \frac{(\log_2 x)^3}{(\log n)^{1/2}}.$$

Taking into account the bound (5) and the combination of [11, Lemmas 2, 3], for $x > x_0$ we see that all but $O(\log_2 x)$ of the triples (U, V_1, V_2) constructed in this manner satisfy the conditions of [11, Lemma 7] if the parameter δ_2 in that lemma is replaced by Δ_2. Following the proof, we conclude that the bound [11, Equation (47)] on the number $t_1 t_2$ of such triples (U, V_1, V_2) can be replaced by

$$t_1 t_2 \leqslant 2^{100\mu^2 s} \qquad (x > x_0)$$

in our situation, where

$$\mu := 2\left\lfloor 3\Delta_2^{-1}\right\rfloor + 1 \qquad \text{and} \qquad s := \omega(k) + 2.$$

As $\mu \leqslant 7\Delta_2^{-1}$ and $s \leqslant 1.1 \log_2 x$ (since $k \notin \mathcal{N}_1(x)$), we see that

$$100\mu^2 s \leqslant 5400\,\frac{\log n}{(\log_2 x)^5} \leqslant \frac{\log n}{3\log 2} - 1 \qquad (x > x_0).$$

Putting everything together, it follows that the Carmichael number $2^n k + 1$ has at most $t_1 t_2 + O(\log_2 x) \leqslant (\frac{1}{2} + o(1))n^{1/3}$ prime divisors $p = 2^m d + 1$ with $m > \Delta_1 N_2$. The result follows. □

2.5 The final argument

We continue to use notation introduced earlier.

Put $z_2 := \lfloor \log_4 x \rfloor$, and let $\mathcal{C}_{11}(x)$ be the set of numbers $k \in \mathcal{C}_{10}^*(x)$ such that $q^2 \mid k$ for some $q > z_2$. For any such q the number of $k \leqslant x$ cannot exceed x/q^2; summing over all q we have

$$|\mathcal{C}_{11}(x)| \leqslant \sum_{q > z_2} \frac{x}{q^2} \ll \frac{x}{z_2} \ll \frac{x}{\log_4 x} = o(x) \qquad (x \to \infty);$$

thus, $\mathcal{C}_{11}(x)$ is a negligible set.

Next, let $\mathcal{C}_{12}(x)$ be the set of $k \in \mathcal{C}_{11}^*(x)$ with the property that there is a prime q such that $q^{z_2} \mid k$. For any such q the number of $k \leqslant x$ does not exceed x/q^{z_2}. Also, since $z_2 > 2$ for $x > x_0$ and $k \notin \mathcal{C}_{11}(x)$, it follows that $q \leqslant z_2$. Consequently,

$$|\mathcal{C}_{12}(x)| \leqslant \sum_{q \leqslant z_2} \frac{x}{q^{z_2}} \leqslant \frac{x \cdot \pi(z_2)}{2^{z_2}} \leqslant \frac{2x \log_4 x}{(\log_3 x)^{\log 2}} = o(x) \qquad (x \to \infty),$$

hence, $\mathcal{C}_{12}(x)$ is negligible.

Finally, we put $\mathcal{C}_{13}(x) := \mathcal{C}_{12}^*(x)$. To complete the proof of Theorem 1 it is enough to show that $\mathcal{C}_{13}(x)$ is negligible. We begin by noting that for every $k \notin \mathcal{N}_1(x)$ the bound

$$n \leqslant K_1 := \exp((\log x)^4)$$

holds whenever $2^n k+1$ is Carmichael; in fact, it is an easy consequence of (2) since $\tau(k) \leqslant (\log x)^{0.8}$ (by (5)) and $\omega(k) \leqslant \Omega(k) \leqslant 1.01 \log_2 x$.

In particular, for every $k \in \mathcal{C}_{13}(x)$ there exists $n \in [X_2, K_1]$ such that $2^n k + 1$ is a Carmichael number. The interval $[X_2, K_1]$ can be covered with at most $O(\log K_1) = O((\log x)^4)$ intervals of the form $[a, 2a)$. Thus, if we denote by $\mathcal{C}_{13}(a; x)$ the set of $k \in \mathcal{C}_{13}(x)$ such that $2^n k + 1$ is a Carmichael number for some $n \in [a, 2a)$, we have

$$|\mathcal{C}_{13}(x)| \ll (\log x)^4 \max_{X_2 \leqslant a \leqslant K_1} |\mathcal{C}_{13}(a; x)|,$$

hence it suffices to show that

$$\max_{X_2 \leqslant a \leqslant K_1} |\mathcal{C}_{13}(a; x)| \ll \frac{x}{(\log x)^5}. \tag{17}$$

From now on, we work to prove (17).

Now, fix $a \in [X_2, K_1]$ and $k \in \mathcal{C}_{13}(a; x)$, and let $n \in [a, 2a)$ be such that $N := 2^n k + 1$ is Carmichael. Let $\mathcal{P}$ denote the set of prime divisors $p = 2^m d + 1$ of N with $m > \Delta_1 N_2$. Put

$$A := \prod_{\substack{p \mid 2^n k+1 \\ p \in \mathcal{P}}} p \qquad \text{and} \qquad B := \frac{2^n k + 1}{A}.$$

Since every prime $p \mid N$ satisfies (12), and $|\mathcal{P}| \leqslant n^{1/3}$ by Lemma 2, we have

$$A \leqslant (2^{5N_2})^{n^{1/3}} = 2^{5n^{5/6}(\log x)^{1/2}} \leqslant 2^{10a^{5/6}(\log x)^{1/2}} \qquad (x > x_0). \tag{18}$$

Put $s := \lfloor \log_2 x \rfloor$ and $z_3 := (\log x)^{0.9}$. We split the prime factors of B into three sets according to the following types:

(i) Primes $p = 2^m d + 1$ of *type I* are those for which either $m \leqslant a^{1/3}$, or p divides $2^{n_j} k_j + 1$ for $j = 1, \ldots, s$, where $k_1, \ldots, k_s$ are distinct numbers in $\mathcal{C}_{13}(a; x)$ and $n_1, \ldots, n_s \in [a, 2a)$;

(ii) Primes $p = 2^m d + 1$ of *type II* have the property that $2^t d + 1$ is a prime factor of B for at most 100 values of t in the interval $[m, m + z_3]$;

(iii) Primes p of *type III* are prime factors of B that are neither of type I nor of type II.

Factor $B = B_I B_{II} B_{III}$, where

$$B_I := \prod_{\substack{p \mid B \\ p \text{ of type } I}} p, \qquad B_{II} := \prod_{\substack{p \mid B \\ p \text{ of type } II}} p \qquad \text{and} \qquad B_{III} := \prod_{\substack{p \mid B \\ p \text{ of type } III}} p.$$

Our approach is to show that primes of type I are small, whereas primes of type II are few in number. As for primes of type III, there may be many for a given k; however, we show that there are only a few such primes on average, and this is sufficient to finish the proof.

Case 1. *Primes of type I.*

Let $p := 2^m d + 1$ be a prime of type I. Since $d \leqslant x$ for all $p \mid B$, in the case that $m \leqslant a^{1/3}$ it is easy to see that

$$m \leqslant M_3 := 10 a^{1/3} \log x \qquad \text{and} \qquad p \leqslant 2^{M_3} \qquad (x > x_0). \tag{19}$$

Our goal is to show that (19) holds for every type I prime. Assuming this result for the moment and using (5), we derive the bound

$$B_I \leqslant \prod_{\substack{m \leqslant M_3 \\ d \mid k}} 2^{M_3} \leqslant 2^{M_3^2 \tau(k)} \leqslant 2^{a^{2/3} (\log x)^3} \qquad (x > x_0). \tag{20}$$

Now suppose that $p := 2^m d + 1$ is of type I with $m > a^{1/3}$, and let $k_1, \ldots, k_s$ and $n_1, \ldots, n_s$ have the properties described in (i). We claim that there are two numbers k_j, say k_1 and k_2, for which there exists a prime q dividing k_2 but not k_1; in particular, since d divides each k_j, q does not divide d. Indeed, suppose on the contrary that every k_j is divisible by the primes $q_1 \ldots, q_t$, which we order by

$$q_1 < \cdots < q_r \leqslant z_2 < q_{r+1} < \cdots < q_t$$

with $0 \leqslant r \leqslant t$. Since $k_j \notin \mathcal{C}_{11}(x) \cup \mathcal{C}_{12}(x)$ for each j, it follows that

$$k_j = q_{r+1} \cdots q_t \prod_{i=1}^{r} q_i^{\alpha_{i,j}} \qquad \text{with} \quad 1 \leqslant \alpha_{i,j} \leqslant z_2 \qquad (1 \leqslant i \leqslant r,\ 1 \leqslant j \leqslant s).$$

As s cannot exceed the number of all such factorizations, we have (using the bound $\pi(u) \leqslant 2u/\log u$ for all large u)

$$\lfloor \log_2 x \rfloor = s \leqslant z_2^r \leqslant z_2^{\pi(z_2)} \leqslant \exp(2z_2) \leqslant (\log_3 x)^2,$$

which is impossible for $x > x_0$. This contradiction proves the claim.

Next, we apply a three-dimensional analogue of the argument used in §2.4 to derive the inequality (12).

Put $N_3 := \lceil (2a)^{1/3} \rceil$. Since $\max\{m, n_1, n_2\} \leqslant 2a = N_3^3$, all numbers of the form $um + vn_1 + wn_2$ with $(u, v, w) \in [0, N_3]^3$ lie in the interval $[0, 3N_3^4]$; as there are $(N_3 + 1)^3$ such triplets (u, v, w), it follows that there exist $(u_1, v_1, w_1) \neq (u_2, v_2, w_2)$ for which

$$\big|(u_1 m + v_1 n_1 + w_1 n_1) - (u_2 m + v_2 n_1 + w_2 n_2)\big| \leqslant \frac{3N_3^4}{(N_3 + 1)^3 - 1} \leqslant 3N_3.$$

Put $(u, v, w) := (u_1 - u_2, v_1 - v_2, w_1 - w_2) \neq (0, 0, 0)$, and note that

$$\max\{|u|, |v|, |w|\} \leqslant N_3, \qquad |um + vn_1 + wn_2| \leqslant 3N_3. \tag{21}$$

In view of the congruences

$$2^m d \equiv -1 \pmod p \qquad \text{and} \qquad 2^{n_j} k_j \equiv -1 \pmod p \qquad (j = 1, 2),$$

we have

$$2^{um+vn_1+wn_2} d^u k_1^v k_2^w \equiv (-1)^{u+v+w} \pmod p.$$

Therefore, p divides the numerator of the rational number

$$G := 2^{um+vn_1+wn_2} d^u k_1^v k_2^w - (-1)^{u+v+w}.$$

We claim that $G \neq 0$. Indeed, suppose on the contrary that $G = 0$. Since dk_1k_2 is odd, it follows that $um + vn_1 + wn_2 = 0$, $u + v + w$ is even, and $d^u k_1^v k_2^w = 1$. Since there is a prime q that divides k_2 but neither k_1 nor d, it follows that $w = 0$, and therefore

$$2^{um+vn_1} d^u k_1^v = (-1)^{u+v}.$$

However, by the arguments of §2.4 we see this relation is not possible unless $(u, v) = (0, 0)$; but this leads to $(u, v, w) = (0, 0, 0)$, which is not allowed. We conclude that $G \neq 0$.

Since p divides the numerator of G, using (21) we derive the bound

$$p \leqslant 2^{|um+vn_1+wn_2|} d^{|u|} k_1^{|v|} k_2^{|w|} + 1 \leqslant 2^{3N_3+1} x^{3N_3} \leqslant 2^{M_3} \qquad (x > x_0).$$

Since $p > 2^m$, this establishes the promised result that (19) holds for every type I prime.

Case 2. *Primes of type II.*

We first observe that every prime factor $p = 2^m d + 1$ of B satisfies

$$m \leqslant \Delta_1 N_2 \leqslant \frac{2a^{1/2}(\log x)^{1/2}(\log_2 x)^{3/2}}{(\log n)^{1/2}} \leqslant M_4 := 2a^{1/2}(\log_2 x)^2, \qquad (22)$$

where we have used the fact that

$$\log n > \log X_2 = \frac{\log x}{\log_2 x}.$$

Let d be fixed and split the interval $[0, M_4]$ into subintervals $\mathcal{I}_j$ of length z_3, where $\mathcal{I}_j := [jz_3, (j+1)z_3)$ for $j = 0, \ldots, \lfloor M_4/z_3 \rfloor$. Every such $\mathcal{I}_j$ contains at most 100 indices m for which $p = 2^m d + 1$ is a type II prime factor of $2^n k + 1$; these primes clearly satisfy

$$p = 2^m d + 1 \leqslant 2^{2M_4} \qquad (x > x_0).$$

Thus, for fixed d we have

$$\prod_{\substack{p \mid B_{II} \\ p = 2^m d + 1}} p \leqslant (2^{2M_4})^{100(M_4/z_3+1)} \leqslant 2^{300M_4^2/z_3} \qquad (x > x_0).$$

Then, taking the product over all divisors d of k, we derive that

$$B_{II} \leqslant 2^{300M_4^2\tau(k)/z_3} \qquad (x > x_0).$$

Finally, using (5) and the definitions of M_4 and z_3, for all $x > x_0$ we have

$$\frac{300M_4^2\tau(k)}{z_3} \leqslant \frac{1200a(\log_2 x)^4(\log x)^{0.8}}{(\log x)^{0.9}} \leqslant \frac{a}{(\log x)^{0.09}} \qquad (x > x_0)$$

hence we obtain the bound

$$B_{\mathit{II}} \leqslant 2^{a/(\log x)^{0.09}} \qquad (x > x_0). \tag{23}$$

Case 3. *Primes of type III*.

Combining the bounds (18), (20) and (23), we have

$$AB_{I}B_{\mathit{II}} \leqslant 2^{10a^{5/6}(\log x)^{1/2}+a^{2/3}(\log x)^{3}+a/(\log x)^{0.09}} \leqslant 2^{a/2} \qquad (x > x_0);$$

therefore, since

$$2^a \leqslant 2^n k + 1 = AB = AB_I B_{\mathit{II}} B_{\mathit{III}},$$

it follows that

$$B_{\mathit{III}} \geqslant 2^{a/2} \qquad (x > x_0). \tag{24}$$

We now adopt the convention that for every $k \in \mathcal{C}_{13}(a;x)$, the number n is chosen to be the least integer in $[a, 2a)$ such that $2^n k + 1$ is a Carmichael number. With this convention in mind, we use the notation $B_{\mathit{III}}(k)$ instead of B_{III} to emphasize that this number depends only on k.

Multiplying the bounds (24) over all $k \in \mathcal{C}_{13}(a;x)$, we get

$$2^{(a/2)|\mathcal{C}_{13}(a;x)|} \leqslant \prod_{k\in\mathcal{C}_{13}(a;x)} B_{\mathit{III}}(k) \leqslant \Bigg(\prod_{p\in\mathcal{B}_a} p\Bigg)^{s}, \tag{25}$$

where we have used $\mathcal{B}_a$ to denote the collection of type *III* primes that divide some $B_{\mathit{III}}(k)$ with $k \in \mathcal{C}_{13}(a;x)$. Note that every prime in $\mathcal{B}_a$ is repeated no more than s times since p is not of type I.

Let $p = 2^m d + 1 \in \mathcal{B}_a$. Since $d \leqslant x$ and $m \geqslant a^{1/3} \geqslant X_2^{1/3} \geqslant 2\log x$ for all $x > x_0$, it follows that $p \leqslant 2^{2m}$. Thus, fixing m and denoting by $\mathcal{D}_{a,m}$ the set of numbers d for which $2^m d + 1 \in \mathcal{B}_a$, it follows that

$$\prod_{d\in\mathcal{D}_{a,m}} (2^m d + 1) \leqslant 2^{2m|\mathcal{D}_{a,m}|} \leqslant 2^{2M_4|\mathcal{D}_{a,m}|},$$

where we used (22) for the second inequality. Taking the product over all values of $m \leqslant M_4$, we have for $x > x_0$:

$$\prod_{p\in\mathcal{B}_a} p \leqslant 2^{2M_4^2 D_a} \qquad \text{with} \quad D_a := \max_{m\leqslant M_4} |\mathcal{D}_{a,m}|. \tag{26}$$

Hence, to get an upper bound for the product in (26), it suffices to find a uniform upper bound for D_a.

Observe that, as the primes in $\mathcal{B}_a$ are not of type *II*, every $d \in \mathcal{D}_{a,m}$ has the property that $2^t d+1$ is prime for at least 100 values of t in the interval $[m, m+z_3]$. Let m be fixed, and let $\lambda_1 < \cdots < \lambda_{100}$ be fixed integers in the interval $[0, z_3]$. We begin by counting the number of $d \leqslant x$ for which the 100 numbers $\left\{2^{m+\lambda_j} d+1 : 1 \leqslant j \leqslant 100\right\}$ are simultaneously prime. By the Brun sieve, the number of such $d \leqslant x$ is

$$O\left(\frac{x}{(\log x)^{100}}\left(\frac{E}{\varphi(E)}\right)^{100}\right), \qquad \text{where} \quad E := \prod_{i<j}(2^{\lambda_j-\lambda_i}-1).$$

Since

$$E \leqslant 2^{100^2 z_3} \leqslant 2^{10^4 \log x} = x^{10^4 \log 2},$$

using the well known bound $u/\varphi(u) \ll \log_2 u$ we have

$$\frac{E}{\varphi(E)} \ll \log_2 E \ll \log_2 x.$$

Hence, for fixed $\lambda_1 < \cdots < \lambda_{100}$ the number of possibilities for d is

$$O\left(\frac{x(\log_2 x)^{100}}{(\log x)^{100}}\right).$$

As the number of choices for $\lambda_1, \ldots, \lambda_{100}$ in $[0, z_3]$ is $\leqslant (z_3+1)^{100} \ll (\log x)^{90}$, it follows that

$$|\mathcal{D}_{a,m}| \ll \frac{x(\log_2 x)^{100}}{(\log x)^{10}}.$$

Consequently,

$$D_a := \max_{m \leqslant M_4} |\mathcal{D}_{a,m}| \leqslant \frac{x}{(\log x)^9} \qquad (x > x_0),$$

and we have

$$2M_4^2 D_a \leqslant \frac{8ax(\log_2 x)^4}{(\log x)^9} \leqslant \frac{ax}{(\log x)^8} \qquad (x > x_0). \tag{27}$$

Inserting estimate (27) into (26), and combining this with (25), we see that

$$2^{(a/2)|\mathcal{C}_{13}(a;x)|} \leqslant 2^{axs/(\log x)^8},$$

and therefore

$$|\mathcal{C}_{13}(a;x)| \leqslant \frac{2xs}{(\log x)^8} \leqslant \frac{x\log_2 x}{(\log x)^8} \qquad (x > x_0).$$

Since this bound clearly implies (17), our proof of Theorem 1 is complete.

3 Proof of Theorem 2

The following statement provides the key to the proof of Theorem 2.

Theorem 4 (Matomäki). *If* $\gcd(b,m) = 1$ *and* b *is a quadratic residue* mod m*, then for all large* x *there are* $\gg_m x^{1/5}$ *Carmichael numbers up to* x *in the arithmetic progression* b mod m.

In the recent preprint [29], Wright extends the previous theorem to remove the condition on b being a quadratic residue modulo m. Precisely, he showed (under $\gcd(b,m) = 1$) that the number of Carmichael numbers up to x that are congruent to b mod m is $\gg x^{\frac{K}{(\log_3 x)^2}}$, for some constant $K > 0$. Using this result would allow a somewhat easier approach to the problem, but we prefer to use Matomäki's Theorem 4, since it gives a better lower bound for the count.

The next proposition illustrates our approach to the proof of Theorem 2.

Proposition 1. *For all large* x*, there are* $\gg x^{1/5}$ *natural numbers up to* x *that are both Sierpiński and Carmichael.*

Proof. In view of Theorem 4, to prove this result it suffices to find coprime b, m such that b is a quadratic residue mod m, and every sufficiently large number in the arithmetic progression b mod m is a Sierpiński number.

Suppose that we can find a finite collection $\mathcal{C} := \{(a_j, n_j; b_j, p_j)\}_{j=1}^N$ of ordered quadruples of integers with the following properties:

(*i*) $n_1, \ldots, n_N$ are natural numbers, and $p_1, \ldots, p_N$ are distinct primes;

(*ii*) every integer lies in at least one of the arithmetic progressions a_j mod n_j;

(*iii*) $p_j \mid 2^{n_j} - 1$ for each j;

(*iv*) $p_j \mid 2^{a_j} b_j + 1$ for each j;

(v) b_j is a quadratic residue mod p_j for each j.

Put $m := p_1 \cdots p_N$, and let $b \in \mathbb{Z}$ be such that $b \equiv b_j \pmod{p_j}$ for each j. Since $p_1, \ldots, p_N$ are distinct primes, is clear from (v) that b is a quadratic residue mod m. Let k be an arbitrary element of the arithmetic progression b mod m that exceeds $\max\{p_1, \ldots, p_N\}$. For every $n \in \mathbb{Z}$ there exists j such that $n \equiv a_j \pmod{n_j}$. For such j, using (iii) and (iv) one sees that $p_j \mid 2^n k + 1$, hence $2^n k + 1$ is composite since $k > p_j$. As this is so for every $n \in \mathbb{Z}$, it follows that k is Sierpiński.

To complete the proof of the theorem it suffices to observe that

$$\begin{aligned}\mathcal{C} := \{&(1,2;1,3),(2,4;1,5),(4,8;1,17),(8,16;1,257),\\ &(16,32;1,65537),(32,64;1,641),(0,64;-1,6700417)\}\end{aligned} \tag{28}$$

is a collection with the properties (i) $-$ (v). □

Proof of Theorem 2. In view of Theorem 4, it suffices to find coprime b, m such that b is a quadratic residue mod m, and every sufficiently large number in the arithmetic progression b mod m is both Sierpiński and Riesel.

Suppose that we can find *two* finite collections $\mathcal{C} := \{(a_j, n_j; b_j, p_j)\}_{j=1}^N$ and $\mathcal{C}' := \{(c_j, m_j; d_j, q_j)\}_{j=1}^M$ such that $\mathcal{C}$ has the properties (i)–(v) listed in Proposition 1, and $\mathcal{C}'$ has the properties:

(vi) $m_1, \ldots, m_N$ are natural numbers, and $q_1, \ldots, q_N$ are distinct primes;

(vii) the union of the arithmetic progressions c_j mod m_j is $\mathbb{Z}$;

($viii$) $q_j \mid 2^{m_j} - 1$ for each j;

(ix) $q_j \mid 2^{c_j} d_j - 1$ for each j;

(x) d_j is a quadratic residue mod q_j for each j.

Furthermore, assume that

(xi) $\gcd(p_1 \cdots p_N, q_1 \cdots q_M) = 1$.

Put $m := p_1 \cdots p_N q_1 \cdots q_M$, and let $b \in \mathbb{Z}$ be such that $b \equiv b_i \pmod{p_i}$ for $i = 1, \ldots, N$ and $b \equiv d_j \pmod{q_j}$ for $j = 1, \ldots, M$. Since all the primes p_i and q_j are distinct, is clear from (v) that b is a quadratic residue mod m. Arguing as in the proof of Proposition 1 we see that every sufficiently large number in the arithmetic progression $b \bmod m$ is both Sierpiński (using (*iii*) and (*iv*)) and Riesel (using (*viii*) and (*ix*)).

Hence, to prove the theorem it suffices to exhibit collections $\mathcal{C}$ and $\mathcal{C}'$ with the stated properties. For this, we take $\mathcal{C}$ to be the collection listed in (28), whereas for $\mathcal{C}'$ we use the collection disclosed in the Appendix. $\square$

4 Proof of Theorem 3

For the second statement of Theorem 3, observe that if $N := 2^n k - 1$ is a Lehmer number, then $\varphi(N) \mid N - 1 = 2(2^{n-1}k - 1)$. For $n \geqslant 2$ this implies that $4 \nmid \varphi(N)$, which is impossible since N is odd, squarefree and composite.

Turning to the first statement of Theorem 3, let us now suppose that $N := 2^n k + 1$ is Lehmer. We can clearly assume that $n \geqslant 150 \log k$, and by Wright [28] we must have $k \geqslant 3$; therefore,

$$1 \leqslant \omega(k) \leqslant \frac{\log k}{\log 3} < \frac{n}{150}. \tag{29}$$

Since every Lehmer number is Carmichael, we can apply the following lemma, which is a combination of [11, Lemmas 2, 3, 4].

Lemma 3. *Suppose that $p = 2^m d + 1$ is a prime divisor of the Carmichael number $N = 2^n k + 1$, where $d \mid k$ and $n > 3 \log k$.*

(*i*) *If $d = 1$, then $m = 2^\alpha$ for some integer $\alpha \geqslant 0$, and $p < k^2$;*

(*ii*) *if $d > 1$ and the numbers $2^m d$ and $2^n k$ are multiplicatively dependent, then $p < 2^{n/3} k^{1/3} + 1$;*

(*iii*) *if $d > 1$ and the numbers $2^m d$ and $2^n k$ are multiplicatively independent, then $m < 7\sqrt{n \log k}$.*

Moreover, N has at most one prime divisor for which (ii) holds.

Let A_1, A_2, A_3 respectively denote the product of the primes $p \mid N$ for each possibility $(i), (ii), (iii)$ in Lemma 3. If $A_1 > 1$ and $p = 2^{2^\alpha} + 1$ is the largest prime dividing A_1, then we have

$$A_1 \leqslant \prod_{j=0}^{\alpha} (2^{2^j} + 1) = 2^{2^{\alpha+1}} - 1 = (p-1)^2 - 1 \leqslant p^2 \leqslant k^4, \tag{30}$$

and clearly Lemma 3 implies that

$$A_2 \leqslant 2^{n/3}k^{1/3} + 1 \leqslant 2^{n/3+1}k^{1/3}. \tag{31}$$

Furthermore, if the prime divisors of A_3 are $p_j := 2^{m_j}d_j + 1$, $j = 1, \ldots, r$, then

$$d_1 \cdots d_r \mid \varphi(A_3) \mid \varphi(N) \mid N - 1 = 2^n k,$$

so we see that $d_1 \cdots d_r \mid k$ and $r \leqslant \omega(k)$. Consequently,

$$A_3 = \prod_{j=1}^{r}(2^{m_j}d_j + 1) \leqslant \prod_{j=1}^{r} 2^{m_j+1}d_j \leqslant 2^{(7\sqrt{n \log k}+1)\omega(k)}k. \tag{32}$$

Combining (30), (31) and (32), it follows that

$$2^n k \leqslant N = A_1A_2A_3 \leqslant 2^{n/3+1+(7\sqrt{n \log k}+1)\omega(k)}k^{16/3}.$$

Taking the logarithm and using the inequalities of (29) we derive that

$$\begin{aligned} n &\leqslant \frac{n}{3} + 1 + \big(7\sqrt{n \log k} + 1\big)\omega(k) + \frac{13 \log k}{3 \log 2} \\ &\leqslant \frac{n}{3} + \big(7\sqrt{n \log k}\,\big)\omega(k) + \frac{19n}{450 \log 2}, \end{aligned}$$

and it follows that

$$n \leqslant 49\left(\frac{2}{3} - \frac{19}{450 \log 2}\right)^{-2}\omega(k)^2 \log k \leqslant 150\,\omega(k)^2 \log k$$

as stated.

5 Appendix A

The collection $\mathcal{C}'$ that is needed for our proof of Theorem 2 (see §3) consists of the quadruples $(c_j, m_j; d_j, q_j)$ disclosed in the following tables.

c_j	m_j	d_j	q_j
0	2	1	3
1	3	4	7
2	5	8	31
6	7	2	127
0	9	1	73
0	15	1	151
14	21	128	337
23	25	4	601
3	25	1576	1801
21	27	64	262657
11	35	58	71
31	35	16	122921
24	45	22473	23311
35	45	393	631

c_j	m_j	d_j	q_j
23	63	55318	92737
2	63	487243	649657
1	70	a_1	p_1
38	75	15604	100801
63	75	4096	10567201
3	81	2269	2593
30	81	69097	71119
47	81	84847359	97685839
5	90	4120594	18837001
89	105	7154	29191
59	105	48124	106681
26	105	48168	152041

$a_1 := 290641821624556480$; $p_1 := 581283643249112959$

c_j	m_j	d_j	q_j
38	135	43817595232267	49971617830801
39	135	41	271
66	135	41811	348031
51	150	1133819953185	1133836730401
29	162	134527	135433
137	162	33554432	272010961
158	175	12419	39551
8	175	30170438	60816001
33	175	a_2	p_2
155	189	1072100	1560007
92	189	a_3	p_3
51	210	247125	664441
179	210	412036	1564921

$a_2 := 311219987433457559260630$

$p_2 := 535347624791488552837151$

$a_3 := 441835582595213504029595 71$

$p_3 := 2076174855442583929707535 27$

c_j	m_j	d_j	q_j
93	225	68316	115201
168	225	111534	617401
183	225	196089342	1348206751
141	225	5524543637190621	13861369826299351
65	270	14107	15121
134	315	465324	870031
44	315	944338	983431
296	315	524288	2972830715596370681022843537840 1
245	405	421858	537841
155	405	794228530486264	11096527935003481
219	405	a_4	p_4
33	450	4714696801	4714696801
143	450	a_5	p_5
231	525	2325	4201
458	525	3644	7351
336	525	108146490	181165951
21	525	a_6	p_6
138	567	a_7	p_7
518	675	a_8	p_8
68	675	a_9	p_9

$a_4 := 5374027197450830037173993714239791208197682$

$p_4 := 17645665556213400107370602081155737281406841$

$a_5 := 27710576967525166105982 2497$

$p_5 := 2819414729537101777586 47201$

$a_6 := 1303895713785017404043599085666596649185928794498 98771616$

$p_6 := 3259855088755275876696070972226675571162211390901 31514801$

$a_7 := 34175792320105064276509598883086470918869640752174548399861885128941214865520182674355385966526465$

$p_7 := 34175792320105064276509600649933535697253970335472049142780400956425111741139140798213387072831489$

$a_8 := 1086551216887830778103354063694$

$p_8 := 1094270085398478390395590841401$

$a_9 := 37588180335625382878389137779484209103 8$

$p_9 := 47039003850347685518062794194276103240 1$

c_j	m_j	d_j	q_j
668	675	128	2842496263188647640089794561760551
68	675	378466	1605151
293	675	31900530	289511839
83	810	2980	9721
141	810	1619	6481
425	810	1113369644664597	1969543281137041
29	945	a_{10}	p_{10}
96	945	a_{11}	p_{11}
96	1575	79759849	82013401
1356	1575	21286182334	32758188751
344	1575	278298838935101950	76641458269269601
233	1575	a_{12}	p_{12}
411	1575	a_{13}	p_{13}
1806	2025	29194	81001
1191	2025	375769199	429004351
1131	2025	a_{14}	p_{14}

$a_{10} := 508359368077097368171047844215098 70$

$p_{10} := 124339521078546949914304521499392241$

$a_{11} := 59062237672015342892330136827234845353476843214908095835470998053274553710744754308864210671730$

$p_{11} := 89371283318924988713544642472309024678004403189516730060412595564942724011446583991926781827601$

$a_{12} := 49991898934986183257626811352173 9$

$p_{12} := 7643849162910052205552429396479 51$

$a_{13} := 4154116394877892908275228737362364927235769068513078276736213794414 82$

$p_{13} := 74583250684814180851161157624056824483225861455070441620435751771655 1$

$a_{14} := 462022372600473167169237015384303310307$

$p_{14} := 20298399822828555544423831770520705345 51.$

6 Appendix B

We conclude with examples of Sierpiński-Carmichael, Riesel-Carmichael, and Sierpiński-Riesel-Carmichael numbers. The idea behind the construction is the same for each of the three examples. We construct a Carmichael number of the form $N = f(t) = (2t+1)(4t+1)(6t+1)$, where each of the factors $2t+1$, $4t+1$ and $6t+1$ is prime. We can then check that N is Carmichael since $2t$, $4t$ and $6t$ are easily seen to be factors of $N-1$. What remains is to construct the coverings necessary to produce Sierpiński or Riesel numbers (or both): we have called the elements in these coverings $(c_j, m_j; d_j, q_j)$ throughout this article. The final step is to solve the congruence $f(t_j) \equiv d_j \pmod{q_j}$. Thus, we have an additional column for t_j in the tables presented below.

Sierpiński-Carmichael number

Let $f(t) = (6t+1)(12t+1)(18t+1)$.

c_j	m_j	d_j	q_j	t_j
1	2	1	3	0
2	4	1	5	0
4	8	1	17	0
8	16	1	257	0
16	32	1	65537	0
0	48	96	97	76
16	24	226	241	42
32	96	655316	2225377	9066929

Now observe that (c_j, m_j) forms a covering, $t = 1034170868575402949878725$ satisfies all the congruences $t_j \pmod{q_j}$, and that $f(t) \equiv d_j \pmod{q_j}$ for each j. Thus, for this value of t, $f(t)$ is Sierpiński. To see that

$f(t) = 14334478632764751022937716817843022018460764753654322423056136891026326316 01$

is also Carmichael, notice that $6t+1 = 6205025211452417699272351$, $12t+1 = 12410050422904835398544701$, and $18t+1 = 18615075634357253097817051$ are all prime, and $f(t) - 1$ is divisible by $6t$, $12t$, and $18t$.

Riesel-Carmichael number

Let $f(t) = (2t+1)(4t+1)(6t+1)$.

c_j	m_j	d_j	q_j	t_j
0	2	1	3	0
0	3	1	7	0
4	9	32	73	1
5	12	11	13	5
7	8	2	17	11
11	18	14	19	11
25	36	13	37	22
11	48	53	97	44
1	36	55	109	28
19	24	32	241	73
3	16	225	257	196
37	48	29	673	210

Again, the congruences $c_j \pmod{m_j}$ form a covering. Moreover, observe that $t = 383045479078858981706118$ satisfies all the congruences $t_j \pmod{q_j}$, and that $f(t) \equiv d_j \pmod{q_j}$ for each j. Thus, for this value of t, $f(t)$ is Riesel. To see that

$f(t) = 269769135448418694374700865023493304999341066049869782236072911309659160\!9$

is also Carmichael, notice that $2t+1 = 766090958157717963412237$, $4t+1 = 1532181916315435926824473$, and $6t+1 = 2298272874473153890236709$ are all prime, and $f(t)-1$ is divisible by $2t$, $4t$, and $6t$.

Sierpiński-Riesel-Carmichael number

Let $f(t) = (2t+1)(4t+1)(6t+1)$.

c_j	m_j	d_j	q_j	t_j
1	2	1	3	0
0	4	4	5	3
6	12	1	13	0
4	9	41	73	8
10	18	10	19	1
2	24	60	241	91
14	36	16	37	14
34	36	105	109	1
38	72	325	433	91
62	72	37713	38737	1256
0	2	1	3	0
0	3	1	7	0
0	5	1	31	0
5	8	8	17	10
1	10	6	11	1
2	15	38	151	32
11	16	32	257	141
3	20	36	41	26
7	30	75	331	196
3	32	57345	65537	51629
9	40	59633	61681	59393
7	48	72	97	54
19	48	641	673	224
59	60	2	61	26
13	60	1028	1321	129
79	80	2	4278255361	1351662299
113	120	128	4562284561	3018421270

In the table above, the congruence $c_j \pmod{m_j}$ in the top part of the table form a covering, and the congruences in the bottom part of the table form a separate covering. The integer

$t = 13389791055454148119921866922357782982738403032220859250823784762964628449\!23$

satisfies all of the congruences $t_j \pmod{q_j}$ in the entire table. Thus, $f(t) \equiv d_j \pmod{q_j}$ for both the top and bottom parts of the table. This implies that $f(t)$ is both Sierpiński (from the top part) and Riesel (from the bottom part). Finally,

$$f(t) = 115229224052855887100756588659264307276443422419402462627311319917631839876768-$$
$$543292399537807831615677851203822707234896300064793740772960178584232868017442980971-$$
$$81018175939793883529668133511379372716751639187700795757514748636 9$$

is Carmichael, since the factors

$$2t+1 = 267795821109082962398437338447155659654768060644417185016475695259292568 9847,$$
$$4t+1 = 535591642218165924796874676894311319309536121288834370032951390518585137 9693, \text{ and}$$
$$6t+1 = 803387463327248887195312015341466978964304181933251555049427085777877706 9539$$

are all prime, and $f(t)-1$ is divisible by $2t$, $4t$, and $6t$.

References

[1] W. Alford, A. Granville, and C. Pomerance, 'There are infinitely many Carmichael numbers,' *Ann. of Math. (2)* **139** (1994), no. 3, 703–722.

[2] W. Banks, 'Carmichael numbers with a square totient,' *Canad. Math. Bull.* **52** (2009), no. 1, 3–8.

[3] W. Banks, 'Carmichael numbers with a totient of the form $a^2 + nb^2$,' *Monatsh. Math.* **167** (2012), no. 2, 157–163.

[4] W. Banks, W. Nevans and C. Pomerance, 'A remark on Giuga's conjecture and Lehmer's totient problem,' *Albanian J. Math.* **3** (2009), no. 2, 81–85.

[5] W. Banks and C. Pomerance, 'On Carmichael numbers in arithmetic progressions,' *J. Aust. Math. Soc.* **88** (2010) no. 3, 313–321.

[6] Y. Bugeaud, P. Corvaja and U. Zannier, 'An upper bound for the g.c.d. of $a^n - 1$ and $b^n - 1$,' *Math. Z.* **243** (2003), 79–84.

[7] Y. Bugeaud and F. Luca, 'A quantitative lower bound for the greatest prime factor of $(ab+1)(ac+1)(bc+1)$,' *Acta Arith.* **114** (2004), 275–294.

[8] Y. Bugeaud, M. Mignotte and S. Siksek, 'Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers,' *Ann. of Math. (2)* **163** (2006), no. 3, 969–1018.

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

[10] R. D. Carmichael, 'On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \bmod P$,' *Amer. Math. Monthly* **19** (1912), no. 2, 22–27.

[11] J. Cilleruelo, F. Luca and A. Pizarro-Madariaga, 'Carmichael numbers in the sequence $\{2^n k + 1\}_{n \geqslant 1}$,' preprint, 2012.

[12] P. Corvaja and U. Zannier, 'On the greatest prime factor of $(ab+1)(ac+1)$,' *Proc. Amer. Math. Soc.* **131** (2003), 1705–1709.

[13] P. Corvaja and U. Zannier, 'A lower bound for the height of a rational function at $\mathcal{S}$-units,' *Monatsh. Math.* **144** (2005), 203–224.

[14] A. Ekstrom, C. Pomerance and D. S. Thakur, 'Infinitude of elliptic Carmichael numbers,' *J. Austr. Math. Soc.* **92** (2012) no. 1, 45–60.

[15] P. Erdős and A. M. Odlyzko, 'On the density of odd integers of the form $(p-1)2^{-n}$ and related questions,' *J. Number Theory* **11** (1979), no. 2, 257–263.

[16] J.–H. Evertse, 'An improvement of the Quantitative Subspace Theorem,' *Compositio Math.* **101** (1996), 225–311.

[17] K. Ford, 'The distribution of integers with a divisor in a given interval,' *Ann. of Math. (2)* **168** (2008), no. 2, 367–433.

[18] S. Hernández and F. Luca, 'On the largest prime factor of $(ab+1)(ac+1)(bc+1)$,' *Bol. Soc. Mat. Mexicana* **9** (2003), 235–244.

[19] D. H. Lehmer, 'On Euler's totient function,' *Bull. Amer. Math. Soc.* **38** (1932), 745–757.

[20] K. Matomäki, 'Carmichael numbers in arithmetic progressions', *J. Aust. Math. Soc.*, to appear.

[21] E. M. Matveev, 'An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II,' *Izv. Ross. Akad. Nauk Ser. Mat.* **64** (2000), 125–180; English transl. in *Izv. Math.* **64** (2000), 1217–1269.

[22] C. Pomerance, 'On the distribution of pseudoprimes,' *Math. Comp.* **37** (1981), 587–593.

[23] C. Pontreau, 'A Mordell-Lang plus Bogomolov type result for curves in G_m^2,' *Monatsh. Math.* **157** (2009), 267–281.

[24] H. Riesel, 'Några stora primtal,' *Elementa* **39** (1956), 258–260.

[25] W. Sierpiński, 'Sur un problème concernant les nombres $k\,2^n+1$,' *Elem. Math.* **15** (1960), 73–74; Corrig. **17** (1962), 85.

[26] G. Tenenbaum, 'Sur la probabilité qu'un entier possède un diviseur dans un intervalle donné,' *Compositio Math.* **51** (1984), 243–263.

[27] P. Turán, 'On a theorem of Hardy and Ramanujan', *J. London Math. Soc.* **9** (1934), 274–276.

[28] T. Wright, 'On the impossibility of certain types of Carmichael numbers,' *Integers* **12** (2012), A31, 1–13.

[29] T. Wright, 'Infinitely many Carmichael numbers in arithmetic progressions,' preprint, 2012.