Carmichael numbers in the sequence $\{2^n k + 1\}_{n \geq 1}$

Javier Cilleruelo
Instituto de Ciencias Matemáticas (CSIC-UAM-UC3M-UCM) and
Departamento de Matemáticas
Universidad Autónoma de Madrid
28049, Madrid, España
franciscojavier.cilleruelo@uam.es

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

Amalia Pizarro-Madariaga
Departamento de Matemáticas
Uinversidad de Valparaiso, Chile
amalia.pizarro@uv.cl

May 22, 2012

1 Introduction

A Carmichael number is a positive integer N which is composite and the congruence $a^N \equiv a \pmod{N}$ holds for all integers a. The smallest Carmichael number is $N = 561$ and was found by Carmichael in 1910 in [6]. It is well–known that there are infinitely many Carmichael numbers (see [1]). Here, we let k be any odd positive integer and study the presence of Carmichael numbers in the sequence of general term $2^n k + 1$. Since it is known [15] that the sequence $2^n + 1$ does not contain Carmichael numbers, we will assume that $k \geq 3$ through the paper. We have the following result.

For a positive integer m let $\tau(m)$ be the number of positive divisors of m. We also write $\omega(m)$ for the number of distinct prime factors of m. For a positive real number x we write $\log x$ for its natural logarithm.

Theorem 1. *Let $k \geq 3$ be an odd integer. If $N = 2^n k + 1$ is Carmichael, then*

$$n < 2^{2\times 10^6 \tau(k)^2 (\log k)^2 \omega(k)}. \tag{1}$$

The proof of Theorem 1 uses a quantitative version of the Subspace Theorem as well as lower bounds for linear forms in logarithms of algebraic numbers.

Besides $k = 1$ there are other values of k for which the sequence $2^n k + 1$ does not contain any Carmichael numbers. Indeed in [2] it has been shown, among other things, that if we put

$$\mathcal{K} = \{k : \ (2^n k + 1)_{n\geq 0} \text{ contains some Carmichael number}\}$$

then $\mathcal{K}$ is of asymptotic density zero. This contrasts with the known fact that the set

$$\{k : \ (2^n k + 1)_{n\geq 0} \text{ contains some prime number}\}$$

is of lower positive density (see [9]). Since $1729 = 2^6 \times 27 + 1$ is a Carmichael number, we have that $27 \in \mathcal{K}$. While Theorem 1 gives us an upper bound on the largest possible n such that $2^n k + 1$ is Carmichael, it is not useful in practice to check if a given k belongs to $\mathcal{K}$. Here, we prove by elementary means the following result.

Theorem 2. *The smallest element of $\mathcal{K}$ is* 27*.*

For the proofs of Theorems 1 and 2, we start with some elementary preliminary considerations concerning prime factors of Carmichael numbers of the form $2^n k + 1$, namely Lemmas 1, 2, 3 and 4. Then we move on to the proofs of Theorem 1 and 2.

2 Preliminary considerations

Here we collect come results about prime factors of Carmichael numbers of the form $2^n k + 1$. There is no lack of generality in assuming that k is odd. We start by recalling Korselt's criterion.

Lemma 1. *N is Carmichael if and only if N is composite, squarefree and $p - 1 \mid N - 1$ for all prime factors p of N.*

Assume now that k is fixed and $N = 2^n k + 1$ is a Carmichael number for some n. By Lemma 1, it follows that

$$2^n k + 1 = \prod_{i=1}^{s} (2^{m_i} d_i + 1), \tag{2}$$

where $s \geq 2$, $1 \leq m_i \leq n$ and d_i are divisors of k such that $p_i = 2^{m_i} d_i + 1$ is prime for $i = 1, \ldots, s$. The prime factors $p = 2^m d + 1$ of N for which $d = 1$ are called Fermat primes. For them, we must have $m = 2^\alpha$ for some integer $\alpha \geq 0$. The next result shows that one can bound the Fermat prime factors of $2^n k + 1$ in terms of k.

Lemma 2. *If $k \geq 3$ is odd and $p = 2^{2^\alpha} + 1$ is a prime factor of the positive integer $N = 2^n k + 1$, then $p < k^2$.*

Proof. If $\alpha = 0$, then $p = 3 < k^2$ because $k \geq 3$. So, we assume that $\alpha \geq 1$. We write $n = 2^\alpha q + r$, where $|r| \leq 2^{\alpha-1}$. Then

$$N = 2^n k + 1 = 2^{2^\alpha q + r} k + 1 \equiv (-1)^q 2^r k + 1 \pmod{p}.$$

It then follows easily that p divides one of $2^{|r|} k \pm 1$ or $k \pm 2^{|r|}$ according to the parity of q and the sign of r. None of the above expressions is zero and the maximum such expression is $2^{|r|} k + 1$. Hence, $p \leq 2^{|r|} k + 1 \leq 2^{2^{\alpha-1}} k + 1$, which implies $2^{2^{\alpha-1}} \leq k$, so $2^{2^\alpha} \leq k^2$. Clearly, the inequality is in fact strict since the left–hand side is even and the right–hand side is odd, so $p = 2^{2^\alpha} + 1 \leq k^2$, and the inequality is again strict since p is prime and k^2 isn't, which completes the proof of the lemma. $\square$

Primes factors $p = 2^m d + 1$ of N for which $2^n k$ and $2^m d$ are multiplicatively dependent play a peculiar role in the subsequent argument. In what follows, we prove that there can be at most one such prime factor.

Lemma 3. *Assume that $p = 2^m d + 1$ is a proper prime divisor of the integer $N = 2^n k + 1$, such that $d \mid k$ and $2^m d$ and $2^n k$ are multiplicatively dependent. Then $p \leq 2^{n/3} k^{1/3} + 1$. Furthermore N has at most a prime factor p such that $p - 1$ and $N - 1$ are multiplicatively dependent.*

Proof. Let ρ be the minimal positive integer such that $2^n k = \rho^u$ for some positive integer u. Since $2^m d$ and $2^n k$ are multiplicatively dependent, it follows that $2^m d = \rho^v$ for some positive integer v. Since $2^m d < 2^n k$, it follows that $v < u$. Furthermore, $\rho^v \equiv -1 \pmod{p}$ and also $\rho^u \equiv -1 \pmod{p}$. This implies easily that $\nu_2(u) = \nu_2(v)$, where $\nu_p(m)$ denotes the exponent of the prime p in the factorization of m. To see this, write $u = 2^{\alpha_u} u_1$, $v = 2^{\alpha_v} v_1$ with u_1, v_1 odd integers and assume, for example, that $\alpha_u < \alpha_v$. We get a contradiction observing that

$$-1 \equiv \rho^{v u_1} \equiv \left(\rho^{2^{\alpha_u} u_1 v_1}\right)^{2^{\alpha_v - \alpha_u}} \equiv \left(\rho^{u v_1}\right)^{2^{\alpha_v - \alpha_u}} \equiv 1 \pmod{p}.$$

Writing $\alpha = \nu_2(u) = \nu_2(v)$, we get that $u = 2^\alpha u_1,\ v = 2^\alpha v_1$ for some odd integers u_1 and v_1. Furthermore, since $p = (\rho^{2^\alpha})^{v_1} + 1$ is prime, it follows that $v_1 = 1$, otherwise p would have $\rho^{2^\alpha} + 1$ as a proper factor. This shows that p is uniquely determined in terms of $2^n k$. Furthermore, since $u_1 \geq 3$, we get that $\rho^{2^\alpha} \leq (2^n k)^{1/3}$, so $p \leq 2^{n/3} k^{1/3} + 1$. $\square$

The next lemma shows that each of the prime factors $p = 2^m d + 1$ of the Carmichael number $N = 2^n k + 1$ for which $2^m d$ and $2^n k$ are multiplicatively independent is small.

Lemma 4. *Assume that $p = 2^m d + 1$ is a prime divisor of the Carmichael number $N = 2^n k + 1$ such that $d > 1$ and $2^n k$ and $2^m d$ are multiplicatively independent. Then*

$$m < 7\sqrt{n \log k} \qquad \textit{whenever} \qquad n > 3 \log k.$$

Proof. Let $p = d2^m + 1$ be the prime factor of $k2^n + 1$. Put $X = n/\log k$. Consider the congruences

$$d2^m \equiv -1 \pmod p \qquad \text{and} \qquad k2^n \equiv -1 \pmod p. \tag{3}$$

Look at the set of numbers

$$\{mu + nv : (u, v) \in \{0, 1, \ldots, \lfloor X^{1/2} \rfloor\}\}.$$

All the numbers in the above set are in the interval $[0, 2nX^{1/2}]$ and there are $(\lfloor X^{1/2} \rfloor + 1)^2 > X$ of them. Thus, there exist $(u_1, v_1) \neq (u_2, v_2)$ such that

$$|(mu_1 + nv_1) - (mu_2 + nv_2)| \leq \frac{2nX^{1/2}}{X - 1} < \frac{3n}{X^{1/2}} = 3\sqrt{n \log k}$$

provided that $X > 3$, which is equivalent to $n > 3 \log k$. We put $u = u_1 - u_2$ and $v = v_1 - v_2$. Then

$$(u, v) \neq (0, 0), \quad \max\{|u|, |v|\} \leq X^{1/2} \quad \text{and} \quad |um + vn| \leq 3\sqrt{n \log k}. \tag{4}$$

We may also assume that $\gcd(u, v) = 1$, otherwise we may replace the pair (u, v) by the pair $(u/\gcd(u, v)), v/\gcd(u, v))$ and then all inequalities (4) are still satisfied. In the system of congruences (3), we exponentiate the first one to u and the second one to v and multiply the resulting congruences getting

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

Thus, p divides the numerator of the rational number

$$2^{um+vn} d^u k^v - (-1)^{u+v}. \tag{5}$$

Let us see that the expression appearing at (5) above is not zero. Assume that it is. Then, since k and d are odd, we get that $um + vn = 0$, $d^u k^v = 1$ and $u + v$ is even. In particular, $(2^m d)^u (2^n k)^v = 1$, which is false because $(u, v) \neq (0, 0)$ and $2^n k$ and $2^m d$ are multiplicatively independent. Thus, the expression (5) is nonzero. Since p is a divisor of the numerator of the nonzero rational number shown at (5), we get, by using also (4), that

$$\begin{aligned} p &\leq 2^{|um+vn|} d^{|u|} k^{|v|} + 1 \leq 2^{1+3\sqrt{n \log k}} k^{2X^{1/2}} \\ &= 2^{1+(3+2/\log 2)\sqrt{n \log k}} < 2^{7\sqrt{n \log k}}, \end{aligned} \tag{6}$$

because $2/\log 2 < 3$, which implies the desired conclusion. $\square$

3 The Quantitative Subspace Theorem

We need a quantitative version of the Subspace Theorem due to Evertse. Let us recall it. Let $M_{\mathbb{Q}}$ be all the places of $\mathbb{Q}$; i.e. the ordinary absolute value and the p-adic absolute value. For $y \in \mathbb{Q}$ and $w \in M_{\mathbb{Q}}$ we put $|y|_w = |y|$ if $w = \infty$ and $|y|_w = p^{-\nu_p(y)}$ if w corresponds to the prime number p. When $y = 0$, we set $\nu_p(y) = \infty$ and $|y|_w = 0$. Then

$$\prod_{y \in M_{\mathbb{Q}}} |y|_w = 1 \qquad \text{holds for all} \qquad y \in \mathbb{Q}^*.$$

Let $M \geq 2$ be a positive integer and define the *height* of the rational vector $\mathbf{y} = (y_1, \ldots, y_M) \in \mathbb{Q}^M$ as follows. For $w \in M_{\mathbb{Q}}$ write

$$|\mathbf{y}|_w = \begin{cases} \left(\sum_{i=1}^M y_i^2\right)^{1/2} & \text{if} \quad w = \infty; \\ \max\{|y_1|_w, \ldots, |y_M|_w\} & \text{if} \quad w < \infty. \end{cases}$$

Set

$$\mathcal{H}(\mathbf{y}) = \prod_{w \in M_{\mathbb{Q}}} |\mathbf{y}|_w.$$

For a linear form $L(\mathbf{y}) = \sum_{i=1}^M a_i y_i$ with $\mathbf{a} = (a_1, \ldots, a_M) \in \mathbb{Q}^M$, we write $\mathcal{H}(L) = \mathcal{H}(\mathbf{a})$.

Theorem 3 (Evertse)**.** *Let $\mathcal{S}$ be a finite subset of $M_{\mathbb{Q}}$ of cardinality s containing the infinite place and for every $w \in \mathcal{S}$ we let $L_{1,w}, \ldots, L_{M,w}$ be M linearly independent linear forms in M indeterminates whose coefficients in $\mathbb{Q}$ satisfy*

$$\mathcal{H}(L_{i,w}) \leq H \qquad \text{for} \quad i = 1, \ldots, M \quad \text{and} \quad w \in \mathcal{S}. \tag{7}$$

Let $0 < \delta < 1$ and consider the inequality

$$\prod_{w \in \mathcal{S}} \prod_{i=1}^{M} \frac{|L_{i,w}(\mathbf{y})|_w}{|\mathbf{y}|_w} < \left(\prod_{w \in \mathcal{S}} |\det(L_{1,w}, \ldots, L_{M,w})|_w \right) \mathcal{H}(\mathbf{y})^{-M-\delta}. \tag{8}$$

There exist linear subspaces $T_1, \ldots, T_{t_1}$ of $\mathbb{Q}^M$ with

$$t_1 \leq \left(2^{60M^2} \delta^{-7M} \right)^s, \tag{9}$$

such that every solution $\mathbf{y} \in \mathbb{Q}^N \backslash \{0\}$ of (8) satisfying $\mathcal{H}(\mathbf{y}) \geq H$ belongs to $T_1 \bigcup \cdots \bigcup T_{t_1}$.

We shall apply Theorem 3 to a certain finite subset of $\mathcal{S}$ of $M_{\mathbb{Q}}$ and certain systems of linear forms $L_{i,w}$ with $i = 1, \ldots, M$ and $w \in \mathcal{S}$. Moreover, in our case the points $\mathbf{y}$ for which (8) holds are in $(\mathbb{Z}^*)^M$. In particular $|\mathbf{y}|_w \leq 1$ will hold for all finite $w \in M_{\mathbb{Q}}$, as well as the inequalities

$$1 \leq \mathcal{H}(\mathbf{y}) \leq \prod_{w \in \mathcal{S}} |\mathbf{y}|_w \leq M \max\{|y_i| : i = 1, \ldots, M\}.$$

Finally, our linear forms will have integer coefficients and will in fact satisfy

$$\det(L_{1,w}, \ldots, L_{M,w}) = \pm 1 \qquad \text{for all} \qquad w \in \mathcal{S}. \tag{10}$$

With these conditions, the following is a straightforward consequence of Theorem 3 above.

Corollary 1. *Assume that (10) is satisfied, that $0 < \delta < 1$, and consider the inequality*

$$\prod_{w \in \mathcal{S}} \prod_{i=1}^{M} |L_{i,w}(\mathbf{y})|_w < M^{-\delta} \left(\max\{|y_i| : i = 1, \ldots, M\} \right)^{-\delta} \tag{11}$$

for some $\mathbf{y} \in (\mathbb{Z}^*)^M$. Then the conclusion of Theorem 3 holds.

4 S-units on curves

We shall also use a result concerning bounds on the number of solutions of a certain type of $\mathcal{S}$-unit equation. Recall that an $\mathcal{S}$-*unit* is a non-zero rational number y such that $|y|_w = 1$ for all $w \notin \mathcal{S}$. The following result is a corollary of Theorem 1.1 in [14].

Theorem 4 (Pontreau)**.** *Let $f(X,Y) \in \mathbb{Q}[X,Y]$ be a polynomial of degree D which is irreducible (over $\mathbb{C}$) and which is not a binomial (i.e., has more than two nonzero coefficients). Then the number of solutions (u,v) of the equation*

$$f(u,v) = 0 \qquad \textit{with} \qquad (u,v) \in \mathcal{S}^2 \tag{12}$$

is bounded above by

$$t_2 \le 2^{104s+51} D^{6s+3} (\log(D+2))^{10s+6}. \tag{13}$$

5 Baker's linear form in logarithms

We need the following theorem due to Matveev (see [13] or Theorem 9.4 in [5]).

Theorem 5. *Let $t \ge 2$ be an integer, $\gamma_1, \ldots, \gamma_t$ be integers larger than 1 and $b_1, \ldots, b_t$ be integers. Put*

$$B = \max\{|b_1|, \ldots, |b_t|\},$$

and

$$\Lambda = \gamma_1^{b_1} \cdots \gamma_t^{b_t} - 1.$$

Then, assuming that $\Lambda \ne 0$, we have

$$|\Lambda| > \exp\left(-1.4 \times 30^{t+3} \times t^{4.5} (1 + \log B)(\log \gamma_1)(\log \gamma_2) \cdots (\log \gamma_t)\right).$$

6 Proof of Theorem 1

Since Theorem 2 is in fact independent of Theorem 1, we shall assume that $k \ge 27$ whenever $N = 2^n k + 1$ is Carmichael. In particular, $\log k > 3$.

From now on we assume that

$$n > 3 \log k. \tag{14}$$

In particular, Lemma 4 holds.

We put $\delta_0 = (2\sqrt{\tau(k)})^{-1}$ and split the prime factors of the Carmichael number $N = 2^n k + 1$ into four subsets as follows:

(1) Fermat primes;

(2) The (at most one) prime $p = 2^m d + 1$ such that $2^m d$ and $2^n k$ are multiplicatively dependent;

(3) The primes $p = 2^m d + 1$ not of type (1) or (2) above with $m < \delta_0\sqrt{n}$;

(4) The remaining primes.

We write N_i for the product of the primes of type i above for $i = 1, 2, 3, 4$. We next find an upper bound for $N_1N_2N_3$. Clearly, writing $p = 2^{2^\alpha} + 1$ for the maximal Fermat prime factor of N, we have that

$$N_1 \le \prod_{\beta=0}^{\alpha}(2^{2^\beta} + 1) = 2^{2^{\alpha+1}} - 1 = (p-1)^2 - 1 < k^4, \tag{15}$$

by Lemma 2. Secondly,

$$N_2 \le 2^{n/3}k^{1/3} + 1 < 2^{n/3}k, \tag{16}$$

by Lemma 3. Further, putting $n_0 = \delta_0\sqrt{n}$, we have

$$\begin{aligned} N_3 \quad &\le \prod_{\substack{1\le m\le n_0\\ d\mid k}} (2^m d + 1) \le \prod_{1\le m\le n_0}\prod_{d\mid k} 2^{m+1}d = \prod_{1\le m\le n_0} 2^{(m+1)\tau(k)}k^{\tau(k)/2} \\ &\le 2^{(n_0+1)(n_0+2)\tau(k)/2+n_0\tau(k)\log k}, \end{aligned} \tag{17}$$

where we used the fact that $1/(2\log 2) < 1$. Assume that the exponent of 2 in (17) is at most $n_0^2\tau(k) = n/4$. This happens if

$$(n_0+1)(n_0+2)\tau(k)/2 + n_0\tau(k)\log k \le n_0^2\tau(k),$$

which is equivalent to

$$2n_0\log k < n_0^2 - 3n_0 - 2.$$

Assuming that $n_0 \ge 2$, the above inequality is implied by $n_0 \ge 4 + 2\log k$, and since $\log k > 3$, the last two inequalities are satisfied when $n_0 > 4\log k$. Recalling the definition of n_0, we deduce that if

$$n > 64\tau(k)(\log k)^2, \tag{18}$$

then (17) implies that

$$N_3 < 2^{n/4}. \tag{19}$$

So, if inequality (18) holds, then by estimates (15), (16) and (19), we get

$$N_1N_2N_2 < k^4(2^{n/3}k)2^{n/4} = 2^{7n/12}k^5 < 2^{7n/12+10\log k} < 2^{2n/3},$$

where the last inequality follows because $5/\log 2 < 10$ and $n > 120\log k$, where the last inequality is implied by (18). Since $N_1N_2N_3N_4 = N > 2^n$, we get that $N_4 > 2^{n/3}$. On the other hand, by Lemma 4, we have that if $p \mid N_4$, then

$$p < 2^{7\sqrt{n\log k}}k + 1 \le 2^{1+\log k+7\sqrt{n\log k}} < 2^{8\sqrt{n\log k}},$$

where the last inequality above is a consequence of (18). Hence,

$$2^{n/3} < N_4 < 2^{8\omega(N_4)\sqrt{n\log k}},$$

showing that

$$\omega(N_4) > \frac{\sqrt{n}}{24\sqrt{\log k}}.$$

We record what we have proved as follows.

Lemma 5. *Assume that*

$$n > 64\tau(k)(\log k)^2. \tag{20}$$

Then there exist at least $\sqrt{n}/(24\sqrt{\log k})$ primes $p = 2^m d+1$ dividing $2^n k+1$ subject to the following properties:

(1) $d > 1$ is a divisor of k;

(2) $\delta_0\sqrt{n} < m < 7\sqrt{n\log k}$;

(3) $2^m d$ and $2^n k$ are multiplicatively independent.

We next take a look at prime divisors $p = d2^m + 1$ of N_4. As we have seen, they have the property that

$$m > n_0 = \delta_0\sqrt{n}. \tag{21}$$

Write

$$n = qm + r, \quad \text{where} \quad 0 \le r \le m-1 < 7\sqrt{n\log k}. \tag{22}$$

Then

$$q = \left\lfloor \frac{n}{m} \right\rfloor \le \frac{n}{m} \le \delta_0^{-1}\sqrt{n} \le 2\sqrt{\tau(k)n}. \tag{23}$$

In congruences

$$k2^{mq+r} \equiv -1 \pmod p \qquad \text{and} \qquad d2^m \equiv -1 \pmod p,$$

raise the second one to power q and divide it out of the first one to get

$$k2^r d^{-q} \equiv (-1)^{q-1} \pmod p.$$

Thus, p divides $d^q + (-1)^q k2^r$. Let us check that this last expression is nonzero. If it were zero, we would then get that $r = 0$, that q is odd, and that $k = d^q$, therefore $2^n k = (2^m d)^q$, which is impossible since $2^n k$ and $2^m d$ are multiplicatively independent. Thus, $d^q + (-1)^q k2^r \neq 0$, and

$$|d^q + (-1)^q k2^r| \ \leq \ 2^r d^q k \leq 2^r k^{q+1} = 2^{r+(q+1)(\log k)/(\log 2)}.$$

Using (22) and (23) we have that

$$\begin{aligned}
r + (q+1)\frac{\log k}{\log 2} &\leq 7\sqrt{n\log k} + (\sqrt{\tau(k)n} + 1)(\log k)/(\log 2) \\
&= \frac{\log k\sqrt{\tau(k)n}}{\log 2}\left(1 + \frac{7\log 2}{\sqrt{\tau(k)\log k}} + \frac{1}{\sqrt{\tau(k)n}}\right) \\
&< \frac{\log k\sqrt{\tau(k)n}}{\log 2}\left(1 + \frac{7\log 2}{\sqrt{\tau(k)\log k}} + \frac{1}{8\tau(k)\log k}\right) \\
&< \frac{\log k\sqrt{\tau(k)n}}{\log 2}\left(1 + \frac{7\log 2}{\sqrt{2\log(27)}} + \frac{1}{16\log(27)}\right) \\
&< 5\log k\sqrt{\tau(k)n}
\end{aligned}$$

Thus, writing $\delta_1 = 5\log k\sqrt{\tau(k)}$, $U = d2^m + 1$ and $V = d^q + (-1)^q k2^r$, we have

$$2^{\delta_0\sqrt{n}} < U \qquad \text{and} \qquad |V| < 2^{\delta_1\sqrt{n}},$$

therefore

$$U > |V|^{\delta_2}, \qquad \text{where} \qquad \delta_2 = \delta_0{\delta_1}^{-1} = (10\tau(k)\log k)^{-1}. \tag{24}$$

We record the following conclusion.

Lemma 6. *Assume that inequality* (20) *is satisfied. Then the number of triples of integers* (U, V_1, V_2) *with the following properties:*

(1) $U = d2^m,\ V_1 = d^q,\ V_2 = (-1)^q k2^r$;

(2) $d > 1$ *is a divisor of* k *and* q *and* r *are nonnegative integers;*

(3) $2^m d$ *and* $2^{mq+r}k$ *are multiplicatively independent;*

(4) $U + 1 \mid V_1 + V_2$*;*

(5) $U > |V_1 + V_2|^{\delta_2}$*;*

exceeds

$$\frac{\sqrt{n}}{24\sqrt{\log k}}.$$

We next find an upper bound for the number of triples (U, V_1, V_2) with the conditions (1)–(5) of Lemma 6 above in terms of k alone.

Lemma 7. *Assume that*

$$n > 10^{28}(\log k)^6 \tau(k). \tag{25}$$

Then the number of triples (U, V_1, V_2) *with the conditions (1)–(5) of Lemma 6 is at most*

$$2^{3\times 61^3 \tau(k)^2 (\log k)^2 \omega(k)}.$$

Proof. We apply Corollary 1. We fix the numbers k and n. The finite set of valuations is

$$\mathcal{S} = \{p \mid 2k\} \cup \{\infty\},$$

so $s = \omega(k) + 2$, where we recall that $\omega(m)$ is the number of distinct prime factors of the positive integer m. The following argument based on the Subspace Theorem is not new. It has appeared before in [3], [4], [7], [8], [12], and perhaps elsewhere. Recall that

$$U = d2^m, \qquad V_1 = d^q \qquad V_2 = (-1)^q k 2^r.$$

Start with

$$\frac{1}{U+1} = \frac{1}{U(1+1/U)} = \frac{1}{U}\left(1 - \frac{1}{U} + \cdots + \frac{(-1)^{N_1-1}}{U^{M_1-1}} + \frac{\zeta_U}{U^{M_1}}\right),$$

where M_1 is a sufficiently large positive integer to be determined later and $|\zeta_U| \le 2$. Thus, we get

$$\left|\frac{1}{1+U} - \frac{1}{U} + \cdots + \frac{(-1)^{M_1}}{U^{M_1}}\right| < \frac{2}{U^{M_1+1}}.$$

Multiply the above inequality by $V = V_1 + V_2$, to get

$$\left| \frac{V}{1+U} - \frac{V_1+V_2}{U} + \cdots + \frac{(-1)^{M_1}(V_1+V_2)}{U^{M_1}} \right| \leq \frac{2|V|}{U^{M_1+1}}.$$

Multiply both sides above by U^{M_1} to get

$$\left| \frac{VU^{M_1}}{1+U} - V_1U^{M_1-1} - V_2U^{M_1-1} + \cdots + (-1)^{M_1}V_1 + (-1)^{M_1}V_2 \right| \leq \frac{2|V|}{U}. \tag{26}$$

We take $M = 2M_1 + 1$ and label the M variables as

$$\mathbf{y} = (y_1, \ldots, y_{2M_1+1}) = (z, y_{1,M_1-1}, y_{2,M_1-1}, \ldots, y_{1,0}, y_{2,0}).$$

We take the linear forms to be

$$L_{1,\infty}(\mathbf{y}) = z - y_{1,M_1-1} - y_{2,M_1-1} + \cdots + (-1)^{M_1-1}y_{1,0} + (-1)^{M_1-1}y_{2,0}$$

and $L_{i,w}(\mathbf{y}) = y_i$ for $(i,w) \neq (1,\infty)$. It is clear that these forms are linearly independent for every fixed $w \in \mathcal{S}$, and condition (10) is satisfied for them. We evaluate the double product

$$\prod_{w\in\mathcal{S}} \prod_{i=1}^{M} |L_{i,w}(\mathbf{y})|_w, \tag{27}$$

when (U, V_1, V_2) are as in Lemma 6,

$$z = \frac{(V_1+V_2)U^{M_1}}{1+U} \quad \text{and} \quad y_{i,j} = V_iU^j \quad (i = 1, 2,\ j = 0, \ldots, M_1 - 1).$$

For $i \geq 2$, y_i is an $\mathcal{S}$-unit and $L_{i,w}(\mathbf{y}) = y_i$ for all $w \in \mathcal{S}$, so that

$$\prod_{w\in\mathcal{S}} \prod_{i=2}^{M} |L_{i,w}(\mathbf{y})|_w = 1. \tag{28}$$

For $i = 1$, since $V/(1+U) \in \mathbb{Z}$, it follows that z is an integer multiple of U^{M_1}. Hence,

$$\prod_{w\in\mathcal{S}\setminus\{\infty\}} \prod_{i=2}^{M} |L_{i,w}(\mathbf{y})|_w \leq U^{-M_1}. \tag{29}$$

Finally, we have

$$|L_{1,\infty}(\mathbf{y})|_\infty \leq \frac{2|V|}{U}, \tag{30}$$

by (26). Multiplying (28), (29) and (30), we get that

$$\prod_{w\in\mathcal{S}}\prod_{i=1}^{M}|L_{i,w}(\mathbf{y})|_w \le \frac{2|V|}{U^{M_1+1}}. \tag{31}$$

Choose $M_1 = \lfloor 3/\delta_2 \rfloor$. Then we have that $M_1 > 2/\delta_2$, therefore

$$U^{M_1} > U^{2/\delta_2} > |V|^2,$$

by (24). Thus,

$$\frac{2|V|}{U^{N_1+1}} < \frac{|V|}{U^{N_1}} \le \frac{1}{|V|}. \tag{32}$$

We now compare $|V|$ and $|V_i|$ for $i = 1, 2$. If q is even, then $V = |V_1| + |V_2|$. Assume now that q is odd. Then

$$|V| = |V_1||k2^r d^{-q} - 1|. \tag{33}$$

By using the inequality of Theorem 5 with $t = 3,\ \gamma_1 = k,\ \gamma_2 = 2,\ \gamma_3 = d,\ b_1 = 1,\ b_2 = r,\ b_3 = -q$, we have that

$$|k2^r d^{-q} - 1| > \exp(-c_1(\log k)^2 \log n), \tag{34}$$

where we used the fact that $\max\{d, k\} \le k$ and $\max\{r, q\} \le n$, and we can take $c_1 = 1.4 \times 30^6 \times 3^{4.5} \times 2 \times \log 2$. Let us check that

$$|k2^r d^{-q} - 1| > U^{-1}. \tag{35}$$

For this, since $U > 2^m > 2^{\delta_0\sqrt{n}}$, it is enough that

$$\delta_0(\log 2)\sqrt{n} > c_1(\log k)^2 \log n,$$

which is equivalent to

$$\frac{\sqrt{n}}{\log(\sqrt{n})} > c_2(\log k)^2\sqrt{\tau(k)}, \tag{36}$$

where $c_2 = 11.2 \times 30^6 \times 3^{4.5}$. Let us spend some time unraveling (36). It is easy to prove that if $A > 3$ then the inequality

$$\frac{x}{\log(x)} > A \quad \text{is implied by} \quad x > 2A\log A.$$

Using this argument it follows that it suffices that

$$\sqrt{n} > 2c_2(\log k)^2\sqrt{\tau(k)}\log\left(c_2(\log k)^2\sqrt{\tau(k)}\right) \tag{37}$$

Since $2\log\log k < \log k$, $\tau(k) < k$ and $\log(c_2) < 28$, we get that

$$\log(c_2) + (\log\tau(k))/2 + 2\log\log k < 28 + 1.5\log k < 11\log k,$$

where the last inequality follows because $\log k > 3$. Hence, in order for (37) to hold, it suffices that

$$\sqrt{n} > 22c_2(\log k)^3\sqrt{\tau(k)},$$

which is satisfied for

$$n > 10^{28}(\log k)^6\tau(k), \tag{38}$$

which is exactly condition (25). Since condition (25) holds, we get that also inequality (35) holds. With (33), we get that

$$|V| = |V_1||k2^r d^{-q} - 1| > |V_1|U^{-1},$$

therefore $|V_1| < |V|U < |V|^2$. A similar argument shows that $|V_2| \le V^2$. Thus, we always have $\max\{|V_1|, |V_2|\} \le |V|^2$ regardless of the parity of q. Hence,

$$\begin{array}{rcl} |V_i|U^{M_1-1} & \le & |V|^2U^{M_1-1} \le |V|^{M_1+1} \qquad (i = 1, 2); \\ \dfrac{|V|U^{M_1}}{1+U} & < & |V|U^{M_1-1} < |V|^{M_1+1}. \end{array}$$

This shows that for our vector $\mathbf{y}$ we have that

$$\max\{|y_i| : i = 1, \ldots, M\} < |V|^{M_1+1}. \tag{39}$$

Finally, we have

$$M = 2M_1 + 1 \le \frac{6}{\delta_2} + 1 < 60\tau(k)\log k + 1 < 2^{\delta_0\sqrt{n}} < U < |V|.$$

Indeed, the middle inequality is equivalent to

$$n > \tau(k)(2\log 2)^2\log^2(60\tau(k)\log k + 1),$$

which is implied by (38). Thus,

$$M\max\{|y_i| : i = 1, \ldots, M\} < |V|^{M_1+2}.$$

Comparing (31) with (32) and the last estimate above, we get

$$\prod_{w\in\mathcal{S}}\prod_{i=1}^{M}|L_{i,w}(\mathbf{y})|_w \le \frac{2|V|}{U^{M_1+1}} \le \frac{1}{|V|} \le (M\max\{|y_i| : i = 1, \ldots, M\})^{-\delta}, \tag{40}$$

where $\delta = 1/(M_1+2)$.

We now apply Corollary 1 with $H = 1$. Note that relation (7) holds for our system of forms, while the condition $\mathcal{H}(\mathbf{y}) \ge 1$ is needed in (i) if obviously fulfilled since $\mathbf{y} \in \mathbb{Z}^M$. We get that all solutions $\mathbf{y}$ to our problem lie in t_1 proper subspaces of $\mathbb{Q}$, where t_1 is bounded as in (9).

Let us take such a subspace. We then get an equation of the form

$$d_0\left(\frac{V_1+V_2}{1+U}\right)U^{M_1} + \sum_{i=1}^{2}\sum_{j=0}^{M_1-1} c_{i,j}V_iU^j = 0 \tag{41}$$

for some vector of coefficients

$$(d_0, c_{i,j} : 1 \le i \le 2, 0 \le j \le M_1 - 1) \in \mathbb{Q}^M$$

not all zero. We divide across equation (41) by $V_1U^{-M_1}$. Further, by setting $W = V_2/V_1 = (-1)^q k 2^r d^{-q}$, we arrive at

$$d_0\frac{W+1}{U+1} + \sum_{i=1}^{2}\sum_{j=0}^{M_1-1} c_{i,j}W^{i-1}U^{-(M_1-j)} = 0.$$

The last equation above is a rational function in the pair (U, W), which is nonzero as a rational function (this has been checked in many places, like [3], or [8], for example). Clearing the denominator $1 + U$, we arrive at an equation of the form

$$\sum_{i=0}^{1}\sum_{j=0}^{M_1} e_{i,j}W^iU^{-j} = 0 \tag{42}$$

for some coefficients $(e_{i,j} : 0 \le i \le 1, 0 \le j \le M_1) \in \mathbb{Q}^M$, not all zero. Put $U_1 = U^{-1}$. The above equation (42) is of the form

$$WP(U_1) + Q(U_1) = 0,$$

where $P(X)$ and $Q(X)$ are in $\mathbb{Q}[X]$ of degrees at most M_1. We distinguish a few cases.

When $P(X) = 0$, then $Q(X) \neq 0$. Then U_1 has at most M_1 values, therefore m is determined in at most M_1 ways.

A similar argument works when $Q(X) = 0$.

Assume now that none of $P(X)$ and $Q(X)$ is the constant zero polynomial. Put

$$F(X, Y) = YP(X) + Q(X).$$

Then any solution (U, W) to equation (42) leads to a solution to the equation $F(U_1, W) = 0$. Assume next that $F(X, Y)$ is a binomial polynomial. It then follows that $P(X) = c_1 X^{f_1}$ and $Q(X) = c_2 X^{f_2}$ for some nonzero rational coefficients c_1, c_2 and some nonnegative integer exponents f_1, f_2. Then since $F(U_1, W) = 0$, it follows that $WU^{f_2 - f_1} = -c_2/c_1$ is uniquely determined. To recover W and U uniquely, we need to check that W and U are multiplicatively independent. If they were not, we would have integers λ and μ not both zero such that

$$|W|^{\lambda} = k^{\lambda} 2^{r\lambda} d^{-q\lambda} = d^{\mu} 2^{m\mu} = U^{\mu}.$$

Hence, we get that $r\lambda - m\mu = 0$, and that $k^{\lambda} = d^{\mu+\lambda}$. If $\lambda = 0$, we then get that $d^{\mu} = 1$, so $\mu = 0$, therefore $(\lambda, \mu) = 0$, which is false. Thus, $\lambda \neq 0$. This leads easily to the conclusion that $2^n k$ and $2^m d$ are multiplicatively dependent (in fact, we get the relation $(2^m d)^{\mu + q\lambda} = (k 2^n)^{\lambda})$, which is not the case. Thus, when $F(X, Y)$ is a binomial polynomial, then there is at most one convenient solution to $F(U_1, W) = 0$.

Assume now that $F(X, Y)$ has at least three nonzero coefficients. Write $P(X) = X^{f_1} P_1(X)$ and $Q(X) = X^{f_2} Q_1(X)$, where $f_1,\ f_2$ are nonnegative integer exponents, and $P_1(X)$ and $Q_1(X)$ are polynomials in $\mathbb{Q}[X]$ with $P_1(0) Q_1(0) \neq 0$. Replace $F(X, Y)$ by

$$\frac{F(X, Y)}{X^{\min\{f_1, f_2\}}} = Y X^{f_1 - \min\{f_1, f_2\}} P_1(X) + X^{f_2 - \min\{f_1, f_2\}} Q_1(X).$$

Then any solution (U, W) to equation (42) still satisfies $F(U_1, V) = 0$ with this new $F(X, Y)$ (because $U_1 \neq 0$). Furthermore, $F(X, Y)$ is now irreducible over $\mathbb{C}[X, Y]$ because it is not divisible by neither X nor Y and it is linear in Y. Its degree D satisfies

$$D \leq \max\{1 + \deg(P_1(X), \deg(P_2(X)\} \leq M_1 + 1 < M.$$

But then, by Theorem 4, the number of solutions (U, W) is at most

$$t_2 \leq 2^{104s+51} M^{6s+3} (\log(M + 2))^{10s+6}. \tag{43}$$

Note that U determines uniquely d and m, which in turn determine also q and r uniquely by (22). To summarize, we get that for fixed n satisfying (38) and odd $k \geq 3$, the number of triples (U, V_1, V_2) with the conditions (1)–(5) of Lemma 6 is at most

$$t_1 t_2,$$

where t_1 and t_2 are shown at (9) and (43), respectively. We now bound t_1 and t_2 for our application.

Note that since $\delta^{-1} = M_1 + 2,\ M = 2M_1 + 1$ and $M_1 = \lfloor 3/\delta_2 \rfloor$, we get easily that

$$\begin{aligned} \delta^{-1} &= (M+3)/2 \\ M &\leq \frac{6}{\delta_2} + 1 \leq 61\tau(k)\log k, && (44) \\ s &= \omega(k) + 2 \leq 3\omega(k). && (45) \end{aligned}$$

Therefore

$$\begin{aligned} t_1 &< (2^{60M^2}\delta^{-7M})^s \\ &< (2^{60M^2}((M+3)/2)^{7M})^s; \end{aligned}$$

and since $s \geq 3$,

$$\begin{aligned} t_2 &< 2^{104s+51}M^{6s+3}(\log(M+2))^{10s+6} && (46) \\ &< \left(2^{221}M^7\log^7(M+2)\right)^s. \end{aligned}$$

Hence,

$$\begin{aligned} t_1t_2 &< \left(2^{60M^2\left(1+\frac{1}{60}\left(\frac{7\log((M+3)/2)}{(\log 2)M}+\frac{221}{M^2}+\frac{7\log M}{(\log 2)M^2}+\frac{7\log\log(M+2)}{(\log 2)M^2}\right)\right)}\right)^s \\ &< 2^{61sM^2} && (47) \end{aligned}$$

provided the quantity

$$E(M) = \frac{7\log((M+3)/2)}{(\log 2)M} + \frac{221}{M^2} + \frac{7\log M}{(\log 2)M^2} + \frac{7\log\log(M+2)}{(\log 2)M^2}$$

satisfies $E(M) < 1$. We observe that

$$\begin{aligned} M &= 2M_1 + 1 = 2\lfloor 3/\delta_2 \rfloor + 1 = 2\lfloor 30\tau(k)\log k \rfloor + 1 \\ &\geq 2\lfloor 30 \times 2 \times \log(27) \rfloor + 1 = 395 \end{aligned}$$

and certainly, $E(M) < 1$ for $M \geq 395$.

Finally, putting (44) and (45) in (47) we get

$$t_1t_2 < 2^{3\times 61^3\omega(k)\tau^2(k)\log^2 k}.$$

□

Theorem 1 follows now from Lemmas 6 and 7. Indeed, observe first that inequality (25) implies inequality (20). Next, assuming that inequality (25), the conclusion of Lemmas 6 and 7 is that

$$\begin{aligned} n &< 24^2(\log k)2^{6\times 61^3\tau(k)^2(\log k)^2\omega(k)} \\ &< 2^{2\times 10^6\tau(k)^2(\log k)^2\omega(k)}, \end{aligned}$$

where we have used that $24^2(\log k) < 2^{\tau(k)^2(\log k)^2\omega(k)}$ for $k \geq 27$.

So, to finish, it suffices to prove that

$$2^{2\times 10^6\tau(k)^2(\log k)^2\omega(k)} > 10^{28}(\log k)^6\tau(k),$$

which follows since $2^x > (10x)^4$ for $x > 100$ with

$$x = 2 \times 10^6\tau(k)^2(\log k)^2\omega(k).$$

7 The proof of Theorem 2

We have to show that if $k \leq 25$ is odd, then there is no Carmichael number of the form $2^n k + 1$. We distinguish five cases, according to whether k is prime, or $k \in \{9, 15, 21, 25\}$.

7.1 $k \leq 23$ is prime

By Lemma 1, we have that if p is a Fermat prime factor of $N = 2^n k + 1$, then $p < k^2 \leq 23^2$, therefore $p \in \{3, 5, 17, 257\}$. By the Main Theorem 2 in [15], we get that there are only seven possibilities for N, namely

$$\begin{aligned} N \in\ & \{5 \times 13 \times 17, 5 \times 13 \times 193 \times 257, 5 \times 13 \times 193 \times 257 \times 769, \\ & 3 \times 11 \times 17, 5 \times 17 \times 29, 5 \times 17 \times 29 \times 113, 5 \times 17 \times 257 \times 509\}. \end{aligned} \tag{48}$$

There is another possibility listed in [15], namely

$$N = 5 \times 29 \times 113 \times 65537 \times 114689,$$

which is not convenient for us since 65537 is a Fermat number exceeding 23^2. However, no number from list (48) is of the form $2^n k + 1$ for some odd prime $k \leq 23$.

7.2 Preliminary remarks about the cases $k \in \{9, 15, 21, 25\}$

We first run a search showing that there is no Carmichael number of the form $2^n k + 1$ for all $n \in \{1, \ldots, 256\}$. Suppose now that $n > 256$. Write

$$2^n k + 1 = \prod_{i=1}^{s} (2^{m_i} d_i + 1)$$

where $1 \le m_i \le n$, $d_i \mid k$ for $i = 1, \ldots, s$ and $p_i = 2^{m_i} d_i + 1$ is prime for all $i = 1, \ldots, s$. We assume that the primes are listed in such a way that

$$a = m_1 \le m_2 \le \cdots .$$

We first show that $n > a + 20$. Indeed, assume that this is not so. If p_1 is a Fermat prime, then, by Lemma 1, we have $a \le (\log k)/\log 2 < 5$, so $n \le a + 20 \le 25$, which is false. If $2^n k$ and $2^{m_1} d_1$ are multiplicatively dependent, then Lemma 2 shows that $a \le n/3$. Thus, $n \le a + 20 \le n/3 + 20$, therefore $n \le 30$, which is again false. Finally, assume that $d_1 > 1$ and $2^{m_1} d_1$ and $2^n k$ are multiplicatively dependent. Then Lemma 3 shows that $a = m_1 < 7\sqrt{n \log k} < 14\sqrt{n}$ because $3 \log k \le 3 \log 27 < 12 < n$. Thus, $n < 14\sqrt{n} + 20$, which is impossible for $n \ge 256$. So, indeed $n > a + 20$. From this, we conclude that if we put b_i such that

$$b_i = \nu_2(p_1 p_2 \cdots p_i - 1)$$

for $i = 1, 2, \ldots, s - 1$ and $b_i \le a + 20$, then $a_{i+1} \le b_i$. This argument will be used in what follows without further referencing.

7.3 $k = 9$

If p is a Fermat number dividing N, then $p \le 9^2 = 81$ by Lemma 1, so $p \in \{3, 5, 17\}$. Clearly, $3 \nmid 2^n \cdot 9 + 1$ for any $n \ge 1$, therefore $p \in \{5, 17\}$. We now write

$$2^n \cdot 9 + 1 = \prod_{i=1}^{s} (2^{a_i} + 1) \prod_{i=1}^{t} (2^{b_i} \cdot 3 + 1) \prod_{i=1}^{u} (2^{c_i} \cdot 9 + 1),$$

where $a_1 < \cdots < a_s$, $b_1 < \cdots < b_t$, $c_1 < \cdots < c_u$. It is easy to see that a_1, b_1, c_1 cannot be all three distinct. Let $a = \min\{a_1, b_1, c_1\}$. We do a case by case analysis according to the number a.

If $a = 1$, the possibilities are that two of $3, 7, 19$ divide N. As we have seen, $3 \nmid N$, so both 7 and 19 divide N. However, 7 never divides $2^n \cdot 9 + 1$, which is a contradiction.

If $a = 2$, then two of $5,\ 13,\ 37$ divide N. However, $5 \mid N$ implies $n \equiv 0 \pmod 4$. Similarly, $13 \mid N$ implies $n \equiv 10 \pmod{12}$, while $37 \mid N$ implies $n \equiv 2 \pmod{36}$, and no two such congruences can simultaneously hold.

If $a = 3$, then $2^3 \cdot 3 + 1 = 25$ is not prime, and we get a contradiction.

If $a = 4$, then neither one of $2^4 \cdot 3 + 1 = 49 = 7^2$ or $2^4 \cdot 9 + 1 = 145 = 5 \times 29$ is prime, again a contradiction.

Thus, $a \geq 5$. In particular, $s = 0$, and $b_1 = c_1$. Put $p_1 = 2^a \cdot 3 + 1$ and $p_2 = 2^a \cdot 9 + 1$. For an odd prime p we put $\mathrm{ord}_p(2)$ for the multiplicative order of 2 modulo p. Then $\mathrm{ord}_2(p_i) = 2^{\alpha_i} \cdot \delta_i$, where $\alpha_i \leq a$ and $\delta_i \in \{1, 3, 9\}$ for $i = 1, 2$. The congruences

$$2^n \cdot 9 \equiv -1 \pmod{p_1} \qquad \text{and} \qquad 2^{2a} \cdot 9 \equiv 1 \pmod{p_1}$$

imply $2^{n-2a} \equiv -1 \pmod{p_1}$, which implies that $\mathrm{ord}_{p_1}(2) \mid 2n - 4a$, therefore $2n \equiv 4a \pmod{2^{\alpha_1}}$. Similarly, from the congruences

$$2^n \cdot 9 \equiv -1 \pmod{p_2} \quad \text{and} \quad 2^a \cdot 9 \equiv -1 \pmod{p_2},$$

we get $2^{n-a} \equiv 1 \pmod{p_2}$, so $n \equiv a \pmod{2^{\alpha_2}}$, or $4n \equiv 4a \pmod{2^{\alpha_2}}$. Thus, putting $\alpha = \min\{\alpha_1, \alpha_2\}$, we get that $2n \equiv 4a \pmod{2^{\alpha}}$ and also $4n \equiv 4a \pmod{2^{\alpha}}$, therefore $2n \equiv 0 \pmod{2^{\alpha}}$. In particular, $2^{\alpha} \cdot 9 \mid 18n$, showing that one of the numbers p_1 or p_2 divides $2^{18n} - 1$. Since

$$p_i \mid 2^n \cdot 9 + 1 \mid 2^{18n} \cdot 9^{18} - 1 = (2^{18n} - 1)9^{18} + (9^{18} - 1)$$

for both $i = 1, 2$, we get that one of p_1 or p_2 divides

$$9^{18} - 1 = 2^4 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37 \cdot 73 \cdot 757 \cdot 530713.$$

However, none of the primes appearing in the right hand side above is of the form $2^a \cdot 3 + 1$ for some $a \geq 5$, which completes the argument in this case.

7.4 $k = 15$

If p is a Fermat number dividing N, then $p < 15^2$, therefore $p \in \{3, 5, 17\}$. Clearly, it is not possible that $3 \mid 2^n \cdot 15 + 1$ or $5 \mid 2^n \cdot 15 + 1$ for any $n \geq 1$, so only $p = 17$ is possible. We write

$$2^n \cdot 15 + 1 = \prod_{i=1}^{s} (2^{m_i} d_i + 1),$$

where $s \geq 2$, $d_i \mid 15$ for $i = 1, \ldots, s$ and $p_i = 2^{m_i} d_i + 1$ is prime for all $i = 1, \ldots, s$. We put again $a = \min\{m_i : i = 1, \ldots, s\}$. Then $p_1 = 2^a d_1 + 1$

and $p_2 = 2^a d_2 + 1$ are both prime divisors of N for two different divisors d_1 and d_2 of 15. We again do a case by case analysis according to the values of a.

If $a = 1$, then $p_1,\ p_2 \in \{7, 11, 31\}$. However, $7 \nmid 2^n \cdot 15 + 1$ for any $n \geq 1$, therefore both 11 and 31 divide N. However, $11 \mid N$ implies that $n \equiv 3 \pmod{10}$, while $31 \mid N$ implies that $n \equiv 1 \pmod 5$, and these two congruences are contradictory.

Assume next that $a = 2$. Since $2^2 \cdot 5 + 1 = 21 = 3 \times 7$ is not prime, it follows that the only possibility is that both 13 and 61 divide N. However, the condition $13 \mid N$ implies that $n \equiv 5 \pmod{12}$, whereas $61 \mid N$ implies that $n \equiv 2 \pmod{60}$, and again the last two congruences for n are contradictory.

The case $a = 3$ is not possible since neither $2^3 \cdot 3 + 1 = 25 = 5^2$ nor $2^3 \cdot 15 + 1 = 121 = 11^2$ is prime.

Assume now that $a = 4$. Since $2^4 \cdot 3 + 1 = 49 = 7^2$ and $2^4 \cdot 5 + 1 = 81 = 3^4$, it follows that the only possibility is that both 17 and 241 divide N. However, the condition $17 \mid N$ implies that $n \equiv 7 \pmod 8$, whereas $241 \mid N$ implies that $n \equiv 4 \pmod{24}$, and these last congruences are again contradictory.

The case $a = 5$ is also impossible since none of $2^5 \cdot 5 + 1 = 161 = 7 \times 23$ and $2^5 \cdot 15 + 1 = 13 \times 37$ is prime.

So, from now on $a_i \geq 6$ for all $i = 1, \ldots, s$. Let $p = 2^b d + 1$ for some $b \geq 6$. Assume that $d = 5$. Since $p \equiv 1 \pmod 8$, it follows that $(-1/p) = (2/p) = 1$, where the above notation is the Legendre symbol. Since $5 \equiv -2^{-b} \pmod p$, it follows that $(5/p) = 1$. Since $3 \equiv -2^{-n} \times 5^{-1} \pmod p$, it follows that $(3/p) = 1$, therefore, by quadratic reciprocity, $(p/3) = 1$, therefore $p \equiv 1 \pmod 3$. However, $2^b \cdot 5 + 1$ is never $1 \pmod 3$ for any positive integer b. This shows that $d \neq 5$. In particular, $d \in \{3, 15\}$ for all prime factors p of N. Assume next that $d = 3$. By a similar argument, we have $(-1/p) = (2/p) = (3/p) = 1$ and now the condition $5 \equiv -2^{-n} \times 3^{-1} \pmod p$ implies that $(5/p) = 1$, which, via quadratic reciprocity, implies that $p \equiv 1, 4 \pmod 5$. Since also $p = 2^b \cdot 3 + 1$, it follows easily that $b \equiv 0 \pmod 4$ (for the values of b congruent to $1, 2, 3$ modulo 4 we get that $2^b \cdot 3 + 1$ is congruent to $2, 3, 0$ modulo 5, respectively, none of which is convenient). Since when $b \equiv 1 \pmod 3$, we have $2^b \cdot 3 + 1$ is a multiple of 7, we get that $b \equiv 0, 2 \pmod 3$, which together with the fact that $b \equiv 0 \pmod 4$, leads to $b \equiv 0,\ 8 \pmod{12}$.

Suppose first that $a \equiv 0 \pmod{12}$. It then follows that the smallest $b > a$ such that $2^b \cdot 3 + 1$ is a prime factor of N is $b \geq a + 8$. Write $p_1 = 2^a \cdot 3 + 1$ and $p_2 = 2^a \cdot 15 + 1$. Then

$$p_1 p_2 = 1 + 2^{a+1}(9 + 2^{a-1} \cdot 45)$$

is a divisor of N. So, $p_3 = 2^{a+1} \cdot 15 + 1$ is also a divisor of N. Thus,

$$\begin{aligned} p_1p_2p_3 &= (1 + 2^{a+1}(9 + 2^{a-1}45))(1 + 2^{a+1} \cdot 15) \\ &= 1 + 2^{a+1}(24 + 2^{a-1} \cdot 45) + 2^{2a+2} \cdot 15(9 + 2^{a-1} \cdot 45) \\ &= 1 + 2^{a+4}(3 + 2^{a-4}M_1) \end{aligned}$$

is a divisor of N, where M_1 is some odd integer. Thus, $p_4 = 2^{a+4} \cdot 15 + 1$ is also a prime factor of N. We then have

$$\begin{aligned} p_1p_2p_3p_4 &= (1 + 2^{a+4}(3 + 2^{a-4} \cdot M_1))(1 + 2^{a+4} \cdot 15) \\ &= 1 + 2^{a+4}(18 + 2^{a-4}M_2) \\ &= 1 + 2^{a+5}(9 + 2^{a-5}M_2), \end{aligned}$$

where M_2 is some odd integer. Thus, $p_5 = 2^{a+5} \cdot 15 + 1$ is also a prime factor of N. However, since $a \equiv 0 \pmod{12}$, it follows that $a + 5 \equiv 5 \pmod{12}$, which implies that $p_5 \equiv 0 \pmod{13}$, a contradiction.

Assume next that $a \equiv 8 \pmod{12}$. Since $2^8 \cdot 15 + 1 = 3841 = 23 \times 167$ is not prime, it follows that $a \geq 20$. We take again $p_1 = 2^a \cdot 3 + 1$ and $p_2 = 2^a \cdot 15 + 1$. Then

$$p_1p_2 = 1 + 2^{a+1}(9 + 2^{a-1} \cdot 45)$$

is a divisor of N. Thus, $p_3 = 2^{a+1} \cdot 15 + 1$ is a divisor of N and

$$\begin{aligned} p_1p_2p_3 &= (1 + 2^{a+1} \cdot 15)(1 + 2^{a+1}(9 + 2^{a-1} \cdot 45)) \\ &= 1 + 2^{a+1}(24 + 2^{a-1}M_1) \\ &= 1 + 2^{a+4}(3 + 2^{a-4}M_1) \end{aligned}$$

is a divisor of N for some odd integer M_1. Since $a + 4 \equiv 0 \pmod{12}$, it follows that either $2^{a+4} \cdot 3 + 1$ is a divisor of N or $2^{a+4} \cdot 15 + 1$ is a divisor of N but not both. In the first case, $p_4 = 2^{a+4} \cdot 3 + 1$ and

$$p_1p_2p_3p_4 = (1 + 2^{a+4} \cdot 3)(1 + 2^{a+4}(3 + 2^{a-4}M_1)) = 1 + 2^{a+5}(3 + 2^{a-5}M_2)$$

is a divisor of N for some odd integer M_2, while in the second case we have $p_4 = 2^{a+4} \cdot 15 + 1$ and

$$p_1p_2p_3p_4 = (1 + 2^{a+4} \cdot 15)(1 + 2^{a+4}(3 + 2^{a-4}M_1)) = 1 + 2^{a+5}(9 + 2^{a-5}M_2)$$

is a divisor of N again for some odd integer M_2. In both cases, we conclude that $p_5 = 2^{a+5} \cdot 15 + 1$ divides N and

$$p_1p_2p_3p_4p_5 = (1 + 2^{a+5} \cdot 15)(1 + 2^{a+5}(T + 2^{a-5}M_2))$$

is a divisor of N for some $T \in \{3, 9\}$. We thus get that

$$p_1p_2p_3p_4p_5 \quad \text{equals} \quad 1 + 2^{a+6}(9 + 2^{a-6}M_3) \quad \text{or} \quad 1 + 2^{a+8}(3 + 2^{a-8}M_3)$$

according to whether $T = 3$ or $T = 9$, respectively. In the first case, we have that $p_6 = 2^{a+6} \cdot 15 + 1$ divides N, whereas in the second case $p_6 = 2^{a+8} \cdot 15 + 1$ divides N. Observe that

$$p_1 \cdots p_6 = (1 + 2^{a+6}(9 + 2^{a-6}M_3))(1 + 2^{a+6} \cdot 15) = 1 + 2^{a+9}(3 + 2^{a-9}M_4)$$

for some odd integer M_4 in the first case, whereas

$$p_1 \cdots p_6 = (1 + 2^{a+8}(3 + 2^{a-8}M_3))(1 + 2^{a+8} \cdot 15) = 1 + 2^{a+9}(9 + 2^{a-9}M_4)$$

in the second case. In either case, $p_7 = 2^{a+9} \cdot 15 + 1$ is a divisor of N. However, since $a \equiv 8 \pmod{12}$, it follows that $a + 9 \equiv 5 \pmod{12}$, so p_7 is a multiple of 13, which is a contradiction.

7.5 $k = 21$

If p is a Fermat factor of N, then $p < 21^2$, therefore $p \in \{3, 5, 17, 257\}$. Clearly, it is not possible that $3 \mid 2^n \cdot 21 + 1$. One also checks that $257 \nmid 2^n \cdot 21 + 1$ for any $n \geq 1$, so only $p = 5, 17$ are possible. We write

$$2^n \cdot 21 + 1 = \prod_{i=1}^{s}(2^{m_i}d_i + 1),$$

where $s \geq 2$, $d_i \mid 21$ for $i = 1, \ldots, s$ and $p_i = 2^{m_i}d_i + 1$ is prime for all $i = 1, \ldots, s$. We put again $a = \min\{m_i : i = 1, \ldots, s\}$. Then $p_1 = 2^a d_1 + 1$ and $p_2 = 2^a d_2 + 1$ are both prime divisors of N for two different divisors d_1 and d_2 of 21. We again do a case by case analysis according to the values of a.

When $a = 1$, we get that two of $2 + 1,\ 2 \cdot 3 + 1,\ 2 \cdot 7 + 1,\ 2 \cdot 21 + 1$ are prime factors of N, which is impossible because $2 + 1 = 3$ and $2 \cdot 3 + 1 = 7$ cannot divide N while $2 \cdot 7 + 1 = 15 = 3 \times 5$ is not prime.

When $a = 2$, we get that two of $2^2+1,\ 2^2{\cdot}3+1,\ 2^2{\cdot}7+1,\ 2^2{\cdot}21+1$. Since $85 = 5 \times 17$ is not prime, it follows that N is divisible by two of $\{5, 13, 29\}$. If $5 \mid N$, then $n \equiv 2 \pmod 4$. If $13 \mid N$, then $n \equiv 3 \pmod{12}$, whereas if 29 $\pmod N$, then $n \equiv 25 \pmod{28}$, and no two of the above congruences are simultaneously possible (the last two imply that $n \equiv 3 \pmod 4$ and $n \equiv 1 \pmod 4$, respectively).

The case $a = 3$ is not possible since neither $2^3 \cdot 3 + 1 = 25 = 5^2$ nor $2^3 \cdot 7 + 1 = 57 = 3 \times 19$ is prime.

From now on, $a \geq 4$. Let $p = 2^b d + 1$ be a prime factor of N. Let us show that d cannot be 7. Assume that it is. Since $b \geq 4$, it follows that $(-1/p) = (2/p) = 1$, and since $7 \equiv -2^{-b} \pmod{p}$, it follows that $(7/p) = 1$. Since also $3 \equiv -2^{-n} \times 7^{-1} \pmod{p}$, it follows that $(3/p) = 1$, so, by quadratic reciprocity, $p \equiv 1 \pmod{3}$. However, $2^b \cdot 7 + 1$ is never congruent to 1 modulo 3, which is a contradiction. Hence, $d \in \{1, 3, 21\}$. Further, suppose that $d = 3$. Then, by the same argument, $(-1/p) = (2/p) = 1$ and so $3 \equiv -2^{-b} \pmod{p}$, therefore $(3/p) = 1$. Since also $7 \equiv -2^{-n} \times 3^{-1} \pmod{p}$, we get that $(7/p) = 1$, which, by quadratic reciprocity, implies that $(p/7) = 1$. Since $p = 2^b \cdot 3 + 1$, it follows that $b \equiv 0 \pmod{3}$ (for b congruent to $1,\ 2$ modulo 3 we get that p is congruent to $0,\ 6$ modulo 7, and none of these possibilities is convenient). Further, in this same instance, it is clear that we cannot have $b \equiv 3 \pmod{4}$, since it would lead to $p = 2^b \cdot 3 + 1$ being a multiple of 5. Hence, $b \equiv 0, 1, 2 \pmod{4}$, which together with $b \equiv 0 \pmod{3}$, leads to $b \equiv 0, 6, 9 \pmod{12}$.

Assume now that $a = 4$. Since $2^4 \cdot 3 + 1 = 49 = 7^2$, it follows that the only possibility is that both 17 and 337 divide N. The condition $17 \mid N$ implies that $n \equiv 2 \pmod{8}$ while the condition that $337 \mid N$ implies that $n \equiv 4 \pmod{21}$. The above conditions imply that $n \equiv 130 \pmod{168}$. Further

$$17 \times 337 = 5729 = 1 + 2^5 \times 179$$

is a divisor of N. It follows that N is divisible by one of $1 + 2^5 \cdot 3 = 97$ or $1 + 2^5 \cdot 21 = 673$. However, there is no $n \geq 0$ such that $97 \mid 2^n \cdot 21 + 1$. Further, $673 \mid N$ implies that $n \equiv 5 \pmod{48}$, which is incompatible with $n \equiv 130 \pmod{168}$ since the first one means that $n \equiv 2 \pmod{3}$, whereas the second one means that $n \equiv 1 \pmod{3}$.

So, from now on we have that $a \geq 5$. Thus, $p_1 = 2^a \cdot 3 + 1$ and $p_2 = 2^a \cdot 21 + 1$. As we have seen, $a \equiv 0 \pmod{3}$. It is also easy to see that $a \equiv 0, 1 \pmod{4}$, otherwise one of $2^a \cdot 3 + 1$ or $2^a \cdot 21 + 1$ is a multiple of 5. Thus, $a \equiv 0, 9 \pmod{12}$.

Now

$$p_1 p_2 = (1 + 2^a \cdot 3)(1 + 2^a \cdot 21) = 1 + 2^a(3 + 21) + 2^{2a} \cdot 63 = 1 + 2^{a+3}(3 + 2^{a-3} \cdot 63).$$

Assume first that $a \equiv 0 \pmod{12}$. Then the next prime factor of N of the form $p = 2^b \cdot 3 + 1$ must have $b \equiv 0, 6, 9 \pmod{12}$, therefore $b \geq a + 6$, so $p_3 = 2^{a+3} \cdot 21 + 1$ must divide N. However, since $a \equiv 0 \pmod{12}$, it follows that p_3 is a multiple of 13. Assume next that $a \equiv 9 \pmod{12}$. In particular,

$a \geq 9$. In fact, since $2^9 \cdot 3 + 1 = 29 \times 53$ is not prime, it follows that $a \geq 21$. Then none of $2^{a+1} \cdot 3 + 1$ and $2^{a+2} \cdot 3 + 1$ are prime factors of N since $a+1$ and $a+2$ are not multiples of 3. Thus, none of $2^{a+1} \cdot 21 + 1$ and $2^{a+2} \cdot 21 + 1$ is a prime factor of N either. Hence, exactly one of $2^{a+3} \cdot 3+1$ or $2^{a+3} \cdot 21+1$ is a prime factor of N. Assume that it is $p_3 = 2^{a+3} \cdot 21 + 1$. Then

$$p_1p_2p_3 = (1 + 2^{a+3}(3 + 2^{a-3} \cdot 69))(1 + 2^{a+3} \cdot 21) = 1 + 2^{a+6}(3 + 2^{a-6}M_1)$$

for some odd integer M_1. Since $a + 4$ and $a + 5$ are not multiples of 3, it follows that none of $2^{a+3} \cdot 3 + 1$ or $2^{a+4} \cdot 3 + 1$ are factors of N, therefore $2^{a+3} \cdot 21 + 1$ and $2^{a+4} \cdot 21 + 1$ are not factors of N either. Hence, one of $2^{a+6} \cdot 3+1$ or $2^{a+6} \cdot 21+1$ is a prime factor of N. Since $a+6 \equiv 3 \pmod{12}$ it follows that the first one cannot be a prime factor of N, whereas the second one is a multiple of 13 so it cannot be prime. So, assume that $p_3 = 2^{a+3} \cdot 3+1$. Then

$$p_1p_2p_3 = (1 + 2^{a+3}(3 + 2^{a-3} \cdot 69)(1 + 2^{a+3} \cdot 3) = 1 + 2^{a+4}(3 + 2^{a-4}M_1)$$

for some odd integer M_1. Since $a + 4$ is not a multiple of 3, it follows that $2^{a+4} \cdot 3 + 1$ is not a prime factor of N, and so $p_4 = 2^{a+4} \cdot 21 + 1$ is a prime factor of N. Observe that

$$p_1p_2p_3p_4 = (1 + 2^{a+4}(3 + 2^{a-4}M_1)(1 + 2^{a+4} \cdot 21) = 1 + 2^{a+7}(3 + 2^{a-7}M_2)$$

for some odd integer M_2. Next, $2^{a+5} \cdot 3 + 1$ are $2^{a+6} \cdot 3 + 1$ are not prime factors of N because $a + 5$ and $a + 6$ are congruent to $2, 3 \pmod{12}$, so $2^{a+5} \cdot 21 + 1$ and $2^{a+6} \cdot 21 + 1$ are not prime factors of N either. Thus, one of $2^{a+7} \cdot 3 + 1$ and $2^{a+7} \cdot 21 + 1$ is a prime factor of N, and since $a + 7$ is not a multiple of 3, it follows that $p_4 = 2^{a+7} \cdot 21 + 1$ is a prime factor of N. Now

$$p_1p_2p_3p_4 = (1 + 2^{a+7}(3 + 2^{a-7}M_2)(1 + 2^{a+7} \cdot 21) = 1 + 2^{a+10}(3 + 2^{a-10}M_3)$$

for some odd integer M_3. Since $a + 8$ is not a multiple of 3, it follows that $2^{a+8} \cdot 3+1$ does not divide N, therefore $2^{a+8} \cdot 21+1$ does not divide N either. If $2^{a+9} \cdot 3 + 1$ is a prime factor of N, then $2^{a+9} \cdot 21 + 1$ is a prime factor of N also, but since $a \equiv 9 \pmod{12}$, it follows that $a + 9 \equiv 2 \pmod 4$, therefore $2^{a+9} \cdot 21 + 1$ is in fact a multiple of 5. Thus, none of $2^{a+9} \cdot 3 + 1$ or $2^{a+9} \cdot 21+1$ is a prime factor of N. Since $a+10$ is not a multiple of 3, we get that $2^{a+10} \cdot 3 + 1$ cannot be a prime factor of N. Thus, $p_5 = 2^{a+10} \cdot 21 + 1$ is a prime factor of N. Thus,

$$p_1 \cdots p_5 = (1+2^{a+10}(3+2^{a-10}M_3))(1+2^{a+10} \cdot 21) = 1+2^{a+13}(3+2^{a-13}M_4)$$

is a divisor of N for some odd integer M_4. Since $a+11$ is not a multiple of 3, it follows that $2^{a+11}\cdot 3+1$ is not a prime factor of N. Therefore $2^{a+11}\cdot 21+1$ is not a prime factor of N either. As for $a+12$, it follows that either both $p_6 = 2^{a+12}\cdot 3+1$ and $p_7 = 2^{a+12}\cdot 13+1$ are prime factors of N, or none of them is. If both of them are, then

$$p_6p_7 = (1+2^{a+12}\cdot 3)(1+2^{a+12}\cdot 21) = 1+2^{a+15}\cdot M_5$$

for some odd integer M_5. So, in either case, namely when both p_5 and p_6 are prime factors of N, or when none of them is, we still infer that one of $2^{a+13}\cdot 3+1$ or $2^{a+13}\cdot 21+1$ is a prime factor of N. However, since $a \equiv 9 \pmod{12}$, $a+13$ is not a multiple of 3, so $2^{a+13}\cdot 3+1$ cannot be a prime factor of N, whereas since $a+13 \equiv 2 \pmod 4$, the number $2^{a+13}\cdot 21+1$ is a multiple of 5, so it cannot be a prime factor of N either. This completes the analysis of the case $k = 21$.

7.6 $k = 25$

If p is a Fermat number dividing N, then $p < 25^2 = 625$, therefore $p \in \{3, 5, 17, 257\}$. Clearly, $5 \nmid 2^n \cdot 25+1$ for any $n \geq 0$, and one can check that $257 \nmid 2^n \cdot 25+1$ for any $n \geq 0$. Thus, $p \in \{3, 17\}$. We now write

$$2^n \cdot 25+1 = \prod_{i=1}^{s}(2^{a_i}+1)\prod_{i=1}^{t}(2^{b_i}\cdot 5+1)\prod_{i=1}^{u}(2^{c_i}\cdot 25+1),$$

where $a_1 < \cdots < a_s,\ b_1 < \cdots < b_t,\ c_1 < \cdots < c_u$. It is easy to see that a_1, b_1, c_1 cannot be all three distinct. Let $a = \min\{a_1, b_1, c_1\}$. We do a case by case analysis according to the number a.

If $a = 1$, then $2\cdot 25+1 = 51 = 3\times 17$ is not prime, so we must have that both 3 and 11 divide $2^n\cdot 25+1$. If $3 \mid 2^n\cdot 25+1$, then $n \equiv 1 \pmod 2$, while if $11 \mid 2^n\cdot 25+1$, then $n \equiv 7 \pmod{10}$. Thus, $33 = 2^5+1$ is a divisor of N. This implies that $b = \min\{a_2, b_2, c_2\} \leq 5$. Put $b = \min\{a_2, b_2, c_2\}$. Assume first that $b < 5$. Then not all three a_2, b_2, c_2 are distinct. The case $b = 2$ is not possible since $2^2+1 = 5$ is not a divisor of N and $2^2\cdot 5+1 = 21 = 3\times 7$ is not prime. The case $b = 3$ is also not possible because $2^3\cdot 25+1 = 201 = 3\times 67$ is not prime. In case $b = 4$, since $2^4\cdot 5+1 = 81 = 3^4$ is not prime, the only possibility is that both $2^4+1 = 17$ and $2^4\cdot 25+1 = 401$. However, $17 \mid N$ implies that $n \equiv 1 \pmod 8$, whereas $401 \mid N$ implies that $n \equiv 4 \pmod{200}$, and these congruences cannot be both satisfied. Thus, $b = 5$. However, this is not possible since none of $2^5\cdot 5+1 = 161 = 7\times 23$ and $2^5\cdot 25+1 = 801 = 3^2\times 89$ is prime.

Assume now that $a = 2$. This is not possible because $2^2 + 1 = 5$ cannot divide N and $2^2 \cdot 5 + 1 = 21 = 3 \times 7$ is not prime.

The case $a = 3$ is not possible because $2^3 \cdot 25 + 1 = 201 = 3 \times 67$ is not prime.

Assume now that $a = 4$. Since $2^4 \cdot 5 + 1 = 81 = 3^4$, it follows that N is divisible by both $2^4 + 1 = 17$ and $2^4 \cdot 25 + 1 = 401$. Again the condition $17 \mid N$ implies that $n \equiv 1 \pmod 8$, whereas $401 \mid N$ implies that $n \equiv 4 \pmod{200}$ and these two congruences cannot simultaneously hold.

From now on, $a \geq 5$, therefore both $2^a \cdot 5 + 1$ and $2^a \cdot 25 + 1$ are prime factors of N, which is false since one of these two numbers is always a multiple of 3.

Acknowledgment. F. L. thanks Jan-Hendrik Evertse for useful advice and for providing some references. This work was done when F. L. and A. P. visited the Mathematical Department and the ICMAT of the UAM in Madrid, Spain, April 2012. These authors thank these institutions for their hospitality and support. During the preparation of this paper. F. L. was also supported in part by Project PAPIIT IN104512 and a Marcos Moshinsky Fellowship. J. C. was supported by Project MTM2011-22851 of the MICINN. A. P. was supported in part by project Fondecyt No. 11100260.

References

[1] W. R. Alford, A. Granville, C. Pomerance (1994). "There are Infinitely Many Carmichael Numbers", *Annals of Mathematics* **139** (1994), 703–722.

[2] W. D. Banks, C. E. Finch, F. Luca, C. Pomerance and P. Stănică, "Sierpiński and Carmichael numbers", *Preprint*, 2012.

[3] 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.

[4] 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.

[5] 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), 969–1018.

[6] R. D. Carmichael, “Note on a new number theory function,” *Bulletin of the American Mathematical Society* **16** (1910), 232–238.

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

[8] 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.

[9] P. Erdős and A. M. Odlyzko, “On the density of odd integers of the form $(p-1)/2^k$ and related questions”, *J. Number Theory* **11** (1979), 257–263.

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

[11] K. Ford, “The distribution of integers with a divisor in a given interval”, *Ann. Math.* **168** (2008), 367–433.

[12] 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.

[13] 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.

[14] C. Pontreau, “A Mordell-Lang plus Bogomolov type result for curves in G_m^2”, *Monatshefte für Mathematik* **157** (2009), 267–281.

[15] T. Wright, “The impossibility of certain types of Carmichael numbers”, *Integers* **12** (2012), #A31.