#A51 INTEGERS 23 (2023)

THERE IS NO CARMICHAEL NUMBER OF THE FORM $2^n p^2 + 1$ WITH p PRIME

Florian Luca
School of Mathematics, University of the Witwatersrand, Wits, South Africa
and
Centro de Ciencias Matemáticas UNAM, Morelia, Mexico
florian.luca@wits.ac.za

Jean Lucien Randrianantenaina
AIMS Cameroon, South West Region, Crystal Gardens, Cameroon
lucien.randrianantenaina@aims-cameroon.org

Received: 5/13/23, Accepted: 7/11/23, Published: 7/21/23

Abstract

In this paper, we prove that there is no Carmichael number of the form $2^n p^2 + 1$ with some integer $n \geq 0$ and prime p.

1. Introduction

A Carmichael number N is a composite positive integer such that the congruence $a^N \equiv a \pmod{N}$ for all integers a. A criterion due to Korselt [3] states that N is Carmichael if and only if N is squarefree, composite and $p - 1 \mid N - 1$ for all $p \mid N$. In particular, $\omega(N) \geq 3$, where $\omega(N)$ is the number of distinct prime factors of N.

Some recent papers investigated Carmichael numbers of the form $2^n k + 1$ for some fixed odd positive integer k. For example, in [2] it is shown that $k \geq 27$ and

$$n < 2^{2\times 10^7 \tau(k)^2 (\log k)^2 \omega(k)},$$

where $\tau(k)$ is the number of divisors of k. In [1], it is shown that there is no Carmichael number of the form $2^n p + 1$ for a prime p.

Here we take this one step further and prove the following theorem.

Theorem 1. *There is no Carmichael number of the form $2^n p^2 + 1$ with p prime.*

DOI: 10.5281/zenodo.8174516

2. The Proof

2.1. Bounding p and n

We follow [1] where it was shown that there is no Carmichael number of the form $2^n p + 1$. We may assume that $n \geq 1$; otherwise $N = p^2 + 1$ is odd, therefore $p = 2$, which is false. Next, $p \geq 3$ since there there is no Carmichael number of the form $2^m + 1$ for any positive integer m. Thus $p^2 \geq 27$, so $p \geq 7$. Since N is Carmichael, it is squarefree and all its prime factors are of the form $q = 2^\lambda p^\delta + 1$ for some integer $\lambda \in [1, n]$ and $\delta \in \{0, 1, 2\}$. When $\delta = 0$, q is a Fermat prime so λ is a power of 2.

So, we may write N as

$$2^n p^2 + 1 = \prod_{j=1}^{r} (2^{\ell_j} + 1) \prod_{j=1}^{s} (2^{n_j} p + 1) \prod_{j=1}^{t} (2^{m_j} p^2 + 1).$$

We have $\omega(N) \geq 3$. Thus, $r + s + t = \omega(N) \geq 3$. We write

$$F_j := 2^{\ell_j} + 1, \qquad P_j := 2^{n_j} p + 1, \qquad \text{and} \qquad Q_j := 2^{m_j} p^2 + 1.$$

We also let

$$F := \prod_{j=1}^{r} F_j, \qquad P := \prod_{j=1}^{s} P_j, \qquad \text{and} \qquad Q := \prod_{j=1}^{t} Q_j.$$

We assume $\ell_1 < \cdots < \ell_r,\ n_1 < \cdots < n_s,\ m_1 < \cdots < m_t$. We need bounds for $F,\ P,\ Q$. The following is Lemma 2 in [2].

Lemma 1. *The inequality $F_j < p^4$ holds for all $j = 1, \ldots, r$.*

In particular, writing $\ell_j = 2^{\alpha_j}$ for $j = 1, \ldots, r$, with $\ell_1 < \cdots < \ell_r$, we have that

$$F = \prod_{j=1}^{r} (2^{2^{\alpha_j}} + 1) \leq (2^{2^{\alpha_r}} + 1)(2^{2^{\alpha_r}} - 1) < F_r^2 < p^8.$$

Lemma 2. *The numbers $P_j - 1$ and $N - 1$ are multiplicatively independent for all $j = 1, \ldots, s$. Further, the numbers $Q_j - 1$ and $N - 1$ are multiplicatively independent for all $j = 1, \ldots, t$.*

Proof. The statement about $Q_j - 1 = 2^{m_j} p^2$ and $N - 1 = 2^n p^2$ is clear since $m_j < n$ for all $j = 1, \ldots, t$. As for $P_j - 1 = 2^{n_j} p$ and $N - 1 = 2^n p^2$, the only chance of them being multiplicatively dependent is when $2 \mid n$ and $n_j = n/2$. But then

$$P_j = 2^{n/2} p + 1 \mid (2^{n/2} p + 1)(2^{n/2} p - 1) = 2^n p^2 - 1 = N - 2$$

implies that P_j divides both N and $N - 2$, so it divides 2, a contradiction. $\square$

Lemma 3. *The inequality* $n_j < 7\sqrt{2n\log p}$ *holds for* $j = 1, \ldots, s$. *Also the inequality* $m_j < 7\sqrt{2n\log p}$ *holds for* $j = 1, \ldots, t$.

Proof. Both inequalities follow from Lemma 4 in [2] except that in that lemma, one needed $n > 6\log p$. So, assume that $m_j \geq 7\sqrt{2n\log p}$ holds for some $j = 1, \ldots, s$. This entails $n < 6\log p$. Since

$$2^{m_j}p^2 + 1 \mid 2^n p^2 + 1$$

entails $n > m_j$, we get

$$n > m_j \geq 7\sqrt{2n\log p} \qquad \text{so} \qquad n > 98\log p,$$

contradicting $n < 6\log p$. A similar argument takes care of $n_j < 7\sqrt{2n\log p}$ for $j = 1, \ldots, s$. Indeed, assume that $n_j \geq 7\sqrt{2n\log p}$ for some $j = 1, \ldots, s$. In particular, $n < 6\log p$. If $t \geq 1$, then

$$2^n p^2 + 1 > (2^{n_j}p + 1)(2p^2 + 1) > 2^{n_j+1}p^3,$$

so

$$n > n_j \geq 7\sqrt{2n\log p} \qquad \text{so} \qquad n > 98\log p,$$

contradicting $n < 6\log p$. So, we may assume that $t = 0$ so $Q = 1$. If $s \geq 2$, then

$$2^n p^2 + 1 \geq (2^{n_j}p + 1)(2p + 1) > 2^{n_j}p^2 + 1,$$

showing that $n > n_j$. Thus, $n > n_j \geq 7\sqrt{2n\log p}$, so again $n > 98\log p$, contradicting the fact that $n < 6\log p$. So, it remains to consider the case when $s = 1$ so $P = P_1 = 2^{n_1}p + 1$. It then follows that $\ell_1 = n_1 \geq 7\sqrt{2n\log p}$. Further,

$$2^n p^2 + 1 = (2^{\ell_1} + 1)\cdots(2^{\ell_r} + 1)(2^{\ell_1}p + 1).$$

Expanding we get that $2^{\min\{\ell_1, \ell_2 - \ell_1\}} \mid p + 1$. In addition, $\lambda(N) = 2^{\ell_r}p$. Here, $\lambda(N)$ is the Carmichael λ-function of N. Recall that for a squarefree positive integer M we have $\lambda(M) = \mathrm{lcm}[p - 1 : p \mid M]$. By Wright's result [4], $p \in \{3, 5, 7, 127\}$ or p is an unknown Fermat prime. In all these cases, $\min\{\ell_1, \ell_2 - \ell_1\} \leq 7$. But $\ell_1 = n_1 \geq 7\sqrt{2n\log p} \geq 7\sqrt{2\log 7} > 13$ is a power of 2 and then ℓ_2 is at least the next power of 2, so $\ell_2 - \ell_1 \geq \ell_1 \geq 13$, a contradiction. $\square$

The next lemmas deal with spacings between the n_js and m_js. For an odd prime P let $O_P := \mathrm{ord}_P(2)$ be the multiplicative order of 2 modulo P.

Lemma 4. *We have* $n - 2n_j \equiv 0 \pmod{o_j}$, *with*

$$o_j := \mathrm{ord}_{P_j}(2)/\gcd(2, \mathrm{ord}_{P_j}(2)).$$

Proof. Well, we have $2^{n_j}p \equiv -1 \pmod{P_j}$ and $2^n p^2 \equiv -1 \pmod{P_j}$. Thus, $2^{n-2n_j} \equiv -1 \pmod{P_j}$. This implies that $O_{P_j} \mid 2(n-2n_j)$, which in turn implies $n - 2n_j \equiv 0 \pmod{o_j}$. □

Lemma 5. *We have $n - m_j \equiv 0 \pmod{O_j}$, where $O_j := \mathrm{ord}_{Q_j}(2)$.*

Proof. Well, we have $2^{n_j}p^2 \equiv -1 \pmod{Q_j}$ and $2^n p^2 \equiv -1 \pmod{Q_j}$. Thus, $2^{n-m_j} \equiv 1 \pmod{P_j}$. This implies that $n - m_j \equiv 0 \pmod{O_j}$. □

We next bound o_j and O_j from below.

Lemma 6. *We have $o_j > 3n_j$ for $1 \le j \le s$ and $O_j > 3m_j$ for $1 \le j \le t$.*

Proof. We start with o_j. Since $o_j = \mathrm{ord}_{P_j}(2)/\gcd(2, \mathrm{ord}_{P_j}(2))$, we have that there is $\varepsilon \in \{\pm 1\}$ such that

$$2^{o_j} \equiv \varepsilon \pmod{P_j}.$$

Thus,

$$2^{o_j} - \varepsilon = (2^{n_j}p + 1)(2^{n'_j}\lambda_j - \varepsilon). \tag{1}$$

Here, $n'_j \ge 1$ and λ_j is odd. We treat the case $\varepsilon = 1$, and $(n'_j, \lambda_j) = (1, 1)$. In this peculiar case we get

$$2^{o_j} - 1 = 2^{n_j}p + 1, \qquad \text{so} \qquad 2^{o_j} = 2(2^{n_j - 1}p + 1),$$

which gives $2^{o_j - 1} = 2^{n_j - 1}p + 1$. This implies $n_j = 1$, and $2^{o_j - 1} = p + 1 \ge 8$, so $o_j \ge 4 > 3n_j = 3$.

From now on, we assume that $(n'_j, \lambda_j) \ne (1, 1)$ when $\varepsilon = 1$. Expanding in (1), we get

$$2^{o_j} = 2^{n_j + n'_j}p\lambda_j + 2^{n'_j}\lambda_j - \varepsilon 2^{n_j}p,$$

and we see that $n_j = n'_j$. Thus,

$$2^{o_j - n_j} = 2^{n_j}p\lambda_j + (\lambda_j - \varepsilon p).$$

Hence, $2^{n_j} \mid \lambda_j - \varepsilon p$. Note that $\lambda_j - \varepsilon p \ne 0$, otherwise $\varepsilon = 1$, $\lambda_j = p$ and $2^{o_j} = 2^{2n_j}p^2$, which is false. In particular, $p + \lambda_j \ge 2^{n_j}$. If $\lambda_j \ge 3$, then $p\lambda_j \ge p + \lambda_j \ge 2^{n_j}$. If $\lambda_j = 1$, then $p\lambda_j = p \ge 2^{n_j} - 1 > 2^{n_j - 0.5}$. The above inequality is true for $n_j \ge 2$. For $n_j = 1$, the inequality $p\lambda_j = p > 2^{n_j - 0.5}$ is also true. Hence,

$$2^{o_j} = (2^{n_j}p + 1)(2^{n_j}\lambda_j - \varepsilon) + \varepsilon > (2^{n_j}p)(2^{n_j - 0.5}\lambda_j) = 2^{2n_j - 0.5}p\lambda_j > 2^{3n_j - 1}.$$

To see the above inequality, note that it is clear when $\varepsilon = -1$, while for $\varepsilon = 1$ we used $2^{n_j}\lambda_j - 1 > 2^{n_j - 0.5}\lambda_j$, which holds since $(n_j, \lambda_j) \ne (1, 1)$. We thus get that $o_j > 3n_j - 1$, so $o_j \ge 3n_j$. Since $o_j \mid P_j - 1 \mid 2^n p^2$ is coprime to 3, we get that $o_j > 3n_j$.

A similar argument works with O_j. In this case, $n \equiv m_j \pmod{O_j}$. Further $2^{O_j} \equiv 1 \pmod{2^{m_j}p^2+1}$. We write

$$2^{O_j} - 1 = (2^{m_j}p^2+1)(2^{m'_j}\lambda_j - 1),$$

with an odd value of λ_j. Expanding, we get

$$2^{O_j} = 2^{m_j+m'_j}p^2\lambda_j - 2^{m_j}p^2 + 2^{m'_j}\lambda_j.$$

Identifying powers of 2 we get $m_j = m'_j$ and further that $2^{m_j} \mid p^2 - \lambda_j$. Note that this last number is nonzero otherwise we have $2^{O_j} = 2^{2m_j}p^4$, which is impossible. Thus, either $p^2 > 2^{m_j}$ or $\lambda_j > 2^{m_j}$. Hence, we get

$$2^{O_j} = (2^{m_j}p^2+1)(2^{m_j}\lambda_j - 1) \geq 2^{2m_j-1}p^2\lambda_j > 2^{3m_j-1}.$$

In the above, we used that $2^{m_j}p^2+1 > 2^{m_j}p^2$ and $2^{m_j}\lambda_j - 1 \geq 2^{m_j-1}\lambda_j$. Thus, $O_j \geq 3m_j$, and since O_j is coprime to 3 (as a divisor of 2^np^2), the inequality is in fact strict. Hence, $O_j > 3m_j$. □

Lemma 7. *We have $n > 2n_j$ for $j = 1.\dots,s$ and $n > m_j$ for $j = 1,\dots,t$.*

Proof. The second one is clear since $2^{m_j}p^2+1 \mid 2^np^2+1$. For the first one, note that $n - 2n_j$ is nonzero, otherwise

$$2^{n_j}p + 1 \mid 2^{2n_j}p^2 + 1,$$

which is not possible. If $2n_j - n > 0$, then since $2n_j - n \equiv 0 \pmod{o_j}$, we get that o_j is a divisor of $2n_j - n$. In particular, $o_j < 2n_j$ contradicting the fact that $o_j > 3n_j$. Thus, it must be the case that $n > 2n_j$. □

We next bound $s,\ t$.

Lemma 8. *We have*

$$s < 3\left(1 + \frac{\log(7\sqrt{2n\log p})}{\log 2.5}\right) \qquad \text{and} \qquad t < 3\left(1 + \frac{\log(7\sqrt{2n\log p})}{\log 2.5}\right).$$

Proof. We show that if X is any number smaller than or equal to $7\sqrt{2n\log p}$, then the interval $[2X/5, X)$ contains at most three numbers of the form n_j for some $j = 1,\dots,s$. Indeed, assume there are four such. Their o_j's are of the form $2^{u_j}p^{\delta_j}$, where $\delta_j \in \{0,1,2\}$. Since we have four numbers, there are two of them say o_j and o'_j having $\delta_j = \delta_{j'}$. In particular, one of $o_j,\ o_{j'}$ divides the other and therefore $o := \min\{o_j, o_{j'}\} = \gcd(o_j, o_{j'})$ is one of o_j or $o_{j'}$. Since $n_j, n'_j \in [2X/5, X)$, we get that $o > 3\min\{n_j, n_{j'}\} \geq 6X/5$. Now

$$n \equiv 2n_j \equiv 2n_{j'} \pmod{o},$$

so that $n_j - n_{j'} \equiv 0 \pmod{o'}$, where $o' := o/\gcd(o,2)$. But

$$|n_j - n_{j'}| < 3X/5 \le o/2 \le o',$$

which shows that $n_j = n_{j'}$, a contradiction.

A similar argument shows that for any positive real number X the interval $[2X/5, X)$ contains at most three of the numbers m_j for $j = 1, \ldots, t$.

Staring with $X := 7\sqrt{2n \log p}$, then each of the intervals

$$[X/2.5, X),\ [X/(2.5)^2, X/2.5), \cdots, [X/(2.5)^{k+1}, X/(2.5)^k),$$

contains at most three values of n_j. Also, each of the above intervals contains at most three values of m_j. If

$$k \ge 1 + \left\lfloor \frac{\log X}{\log 2.5} \right\rfloor > \frac{\log X}{\log 2.5},$$

then $X/(2.5)^k < 1$, so the last interval is contained in $(0,1)$ so it cannot contain any n_j or m_j. This shows that

$$k \le \left\lfloor \frac{\log X}{\log 2.5} \right\rfloor.$$

Thus,

$$s \le 3(k+1) \le 3\left(\left\lfloor \frac{\log(7\sqrt{2n\log p})}{\log 2.5} \right\rfloor + 1\right) < 3\left(1 + \frac{\log(7\sqrt{2n\log p})}{\log 2.5}\right),$$

and also

$$t < 3\left(1 + \frac{\log(7\sqrt{2n\log p})}{\log 2.5}\right).$$

□

Now

$$\begin{aligned} P &= \prod_{j=1}^{s}(2^{n_j}p + 1) \\ &< 2^{3X\sum_{j\ge1}(2/5)^{-j}} p^s \prod_{j\ge1}\left(1 + \frac{1}{2^j p}\right)^3 \\ &< 1.3^3 \cdot 2^{35\sqrt{2n\log p} + 3(1+\log(7\sqrt{2n\log p})/\log 2.5)(\log p/\log 2)}. \end{aligned}$$

In the above we used that

$$3X\sum_{j\ge0}(2.5)^{-j} = \frac{3X}{1 - 1/2.5} = 5X = 35\sqrt{2n\log p},$$

as well as

$$\prod_{j\geq 1}\left(1+\frac{1}{2^j p}\right) < \exp\left(\sum_{j\geq 1}\frac{1}{2^j p}\right) < \exp(1/p) < \exp(1/5) < 1.3.$$

Similarly,

$$Q = \prod_{j=1}^{t}(2^{m_j}p^2+1) < 1.3^3 \cdot 2^{35\sqrt{2n\log p}+3(1+\log(7\sqrt{2n\log p})/\log 2.5)(2\log p/\log 2)}.$$

We record this as the following lemma.

Lemma 9. *We have*

$$\begin{array}{rcl} P & < & 1.3^3 \cdot 2^{35\sqrt{2n\log p}+3(1+\log(7\sqrt{2n\log p})/\log 2.5)(\log p)/(\log 2)}; \\ Q & < & 1.3^3 \cdot 2^{35\sqrt{2n\log p}+3(1+\log(7\sqrt{2n\log p})/\log 2.5)(2\log p)/(\log 2)}. \end{array}$$

Now we put everything together and use that

$$n\log 2 = \log(2^n) < \log N < \log F + \log P + \log Q$$

to get the following result.

Lemma 10. *The inequality*

$$\begin{array}{rcl} n\log 2 & < & 8\log p + 6\log(1.3) + (70\log 2)\sqrt{2n\log p} \\ & + & \left(1+\dfrac{\log(7\sqrt{2n\log p})}{\log 2.5}\right)(9\log p). \end{array} \tag{2}$$

holds.

Lemma 11. *It is not possible that all o_j (for $1 \leq j \leq s$) and O_j (for $1 \leq j \leq t$) are coprime to p.*

Proof. Assume all o_j $(1 \leq j \leq s)$ and O_j $(1 \leq j \leq t)$ are powers of 2. Let b be maximal such that $2^b \leq n/2$. We show:

(i) $O_j/2 \leq 2^b$ for $j = 1, \ldots, t$;

(ii) $\ell_r \leq 2^b$ for $j = 1, \ldots, r$;

(iii) $o_j \leq 2^b$ for $j = 1, \ldots, s$ with at most one exception j which then is unique, has $o_j = 2^{b+1}$ and $n = 2n_j + o_j$.

We start with (i). We have

$$n - m_j \equiv 0 \pmod{O_j}.$$

Clearly, $2^n p^2 + 1 > 2^{m_j} p^2 + 1$ so $n > m_j$. Thus, $O_j < n$, and so $O_j/2 < n/2 \leq 2^b$.

We next deal with (ii). We have $2^{\ell_r} + 1 \mid N$, so $2^{\ell_r} = F_r - 1 \mid N - 1 = 2^n p^2$ showing that $\ell_r \leq n$. We need to show that $\ell_r \leq n/2$. Assume $\ell_r > n/2$. Write

$$2^n p^2 + 1 = (2^{\ell_r} + 1)(2^a \lambda + 1),$$

for some integers $a \geq 1$ and λ odd. Thus,

$$2^n p^2 = 2^{\ell_r + a}\lambda + 2^{\ell_r} + 2^a \lambda,$$

and by inspecting the power of 2 we get $a = \ell_r$. Thus,

$$2^n p^2 = 2^{2\ell_r}\lambda + 2^{\ell_r}(\lambda + 1).$$

Since $2\ell_r > n$, we get that $\ell_r = n$. Next, if $t \geq 1$, then

$$(2^n p^2 + 1) > (2^{\ell_r} + 1)(2p^2 + 1) = (2^n + 1)(2p^2 + 1) > 2^n p^2 + 1,$$

a contradiction. Thus, $t = 0$ so $Q = 1$. It follows that $s \geq 1$. If $s \geq 2$, then

$$2^n p^2 + 1 \geq (2^{\ell_r} + 1)(2p + 1)(4p + 1) = (2^n + 1)(2p + 1)(4p + 1) > 2^n p^2 + 1$$

a contradiction. Thus, $s = 1$ and

$$2^n p^2 + 1 = (2^{\ell_1} + 1) \cdots (2^n + 1)(2^{n_1} p + 1).$$

We get $2^{n - 2n_1} \equiv -1 \pmod{2^{n_1} p + 1}$. So, $n - 2n_1 \equiv o_1 \pmod{2o_1}$, and $o_1 \leq n$ is a power of 2. Since n is a power of 2 which is at least o_1, we get that $o_1 \mid n$ and since $o_1 \mid n - 2n_1$, we get that $o_1 \mid 2n_1$, contradicting the fact that $o_1 > 3n_1$. This shows that $\ell_r \leq n/2$.

We now deal with (iii). We have $n - 2n_j \equiv 0 \pmod{o_j}$. If $o_j \leq n/2$, we have what we want. Assume $o_j > n/2$. Then $n - 2n_j = m o_j$ with some positive integer m together with the fact that $o_j > n/2$ implies that $m = 1$. Thus, $o_j = 2^{b+1}$ is the only power of 2 in $[n/2, n)$ and $n_j = (n - o_j)/2$. Hence, o_j and j are unique.

To finish, assume first that $O_j/2$ $(1 \leq j \leq t)$, ℓ_r and o_j $(1 \leq j \leq s)$ are all powers of 2 of exponent at most b. Then since

$$2^{o_j} + 1 \equiv 0 \pmod{P_j} \quad (1 \leq j \leq s) \quad 2^{O_j/2} + 1 \equiv 0 \pmod{Q_j} \quad (1 \leq j \leq t),$$

we get

$$2^n p^2 + 1 \mid \prod_{0 \leq a \leq b} (2^{2^a} + 1) = 2^{2^{b+1}} - 1 < 2^n,$$

a contradiction. Assume next that there is one j in $\{1,\ldots,s\}$ such that $o_j = 2^{b+1}$ and $n = 2n_j + o_j$. Then

$$\begin{aligned} 2^{2n_j+o_j}p^2+1 &= 2^n p^2+1 \mid (2^{n_j}p+1)\prod_{0\le a\le b}(2^{2^a}+1) \\ &= (2^{n_j}p+1)(2^{2^{b+1}}-1) < (2^{n_j}p+1)2^{o_j}, \end{aligned}$$

which gives

$$2^{2n_j}p^2 \le 2^{n_j}p,$$

a contradiction. This finishes the proof of this lemma. $\square$

Lemma 11 is good news since it shows that one of o_j, O_j is a multiple of p and since $n-2n_j$ and $n-m_j$ are positive integers which are multiples of o_j (for $1\le j\le s$) and O_j respectively (for $1\le j\le t$), we conclude that $n>p$. Inequality (2) now gives

$$\begin{aligned} \log 2 &< \frac{8\log p}{p}+\frac{6\log(1.3)}{p}+(70\log 2)\sqrt{\frac{2\log p}{p}} \\ &+ \left(\frac{1}{\sqrt{p}}+\frac{\log(7\sqrt{2p\log p})}{\sqrt{p}\log 2.5}\right)\left(\frac{9\log p}{\sqrt{p}}\right). \end{aligned}$$

The above gives $p<120000$. But we can do a bit better. That is, assume first that $n\ge p^2$. Then inequality (2) gives

$$\begin{aligned} \log 2 &< \frac{8\log p}{p^2}+\frac{6\log(1.3)}{p^2}+(70\log 2)\sqrt{\frac{2\log p}{p^2}} \\ &+ \left(\frac{1}{p}+\frac{\log(7\sqrt{2p^2\log p})}{p\log 2.5}\right)\left(\frac{9\log p}{p}\right), \end{aligned}$$

which implies $p\le 233$. With this value of p, inequality (2) gives

$$n<55010.$$

Assume next that $n<p^2$. We now revisit Lemma 8 but keep in mind that since $n<p^2$, we must have that o_j, O_j are of the form $2^{\lambda_j}p^{\delta_j}$, where $\delta_j\in\{0,1\}$. That argument shows that in fact the inequalities of Lemma 8 hold with the factor of 2 on the right–hand side instead of 3 and in fact even (2) holds with the right–hand side scaled by a factor of 2/3. This can be rewritten as

$$\begin{aligned} \frac{3n\log 2}{2} &< 8\log p+6\log(1.3)+(70\log 2)\sqrt{2n\log p} \\ &+ \left(1+\frac{\log(7\sqrt{2n\log p})}{\log 2.5}\right)(9\log p). \end{aligned} \tag{3}$$

Since $n > p$, we get

$$\begin{aligned}\frac{3\log 2}{2} &< \frac{8\log p}{p} + \frac{6\log(1.3)}{p} + (70\log 2)\sqrt{\frac{2\log p}{p}}\\ &+ \left(\frac{1}{\sqrt{p}} + \frac{\log(7\sqrt{2p\log p})}{\sqrt{p}\log 2.5}\right)\left(\frac{9\log p}{\sqrt{p}}\right),\end{aligned}$$

which gives $p < 50000$. With this value of p, inequality (3) gives

$$n < 50000.$$

Let us summarize our numerical conclusions.

Lemma 12. *We have $p < 50000$ and $n < 55010$.*

It remains to do the numerics. Since $p < 50000$, we get that

$$F_j < p^2 < 10^{10},$$

so $F_j \in \{3, 5, 17, 257, 65537\}$.

2.2. The Case $F > 1$

Assume $F > 1$. Then $p \mid F - 1$. Since $p < 50000$, the only possibilities are

$$p \in \{7, 11, 13, 19, 29, 31, 41, 43, 47, 83, 107, 113, 127, 131, 151,$$
$$241, 331, 467, 2579, 6553, 10631, 13159, 19661, 45083\}.$$

We start with the large primes.

`The case` $p = 45083$. The only possibility is $F = F_1F_3F_4 = 5 \cdot 257 \cdot 65537$. This is not convenient since none of $2p+1, 2p^2+1, 4p+1, 4p^2+1$ is prime.

`The case` $p = 19661$. The only possibility is $F = F_0 \cdot F_4 = 3 \cdot 65537$. Since $2p^2+1$ is not prime, it follows that $P_1 = 2p+1,\ F_1 = 3$. Then $2^np^2+1 \equiv 0 \pmod{65537}$. The order of 2 modulo 65537 is 32 and a short calculation shows that $2^ip^2+1 \not\equiv 0 \pmod{65537}$ for all $i = 0, \ldots, 31$.

`The case` $p = 13159$. The only possibility is $F = F_0F_2F_4 = 3 \cdot 17 \cdot 65537$. This is not convenient since neither $2p+1$ nor $2p^2+1$ is prime.

`The case` $p = 10631$. The only possibility is $F = F_1F_2F_4 = 5 \cdot 17 \cdot 65537$. This is not convenient since neither of $2p+1, 2p^2+1, 4p+1, 4p^2+1$ is prime.

`The case` $p = 6553$. In this case $F = F_0F_2F_3 = 3 \cdot 17 \cdot 257$. This is not convenient since both $2p+1,\ 2p^2+1$ are composite.

`The case` $p = 2579$. In this case $F = F_2F_4 = 17 \cdot 65537$. This is not convenient since neither one of $2p+1, 2p^2+1, 4p+1, 4p^2+1, 8p+1, 8p^2+1, 16p+1, 16p^2+1$ is prime.

`The case` $p = 467$. In this case, $F = F_1F_3F_4 = 5 \cdot 257 \cdot 65537$. This is not convenient since neither of $2p+1, 2p^2+1, 4p+1, 4p^2+1$ is prime.

`The case` $p = 331$. In this case $F = F_1F_2F_3F_4 = 5 \cdot 17 \cdot 257 \cdot 65537$. This is not convenient since neither of $2p+1, 2p^2+1, 4p+1, 4p^2+1$ is prime.

`The case` $p = 241$. In this case $F = F_3F_4 = 257 \cdot 65537$. This is not convenient since neither of

$$2p+1,\ 2p^2+1,\ 4p+1,\ 4p^2+1,\ 8p+1,\ 8p^2+1,\ 16p+1,\ 16p^2+1,$$

$$32p+1,\ 32p^2+1,\ 64p+1,\ 64p^2+1,\ 128p+1,\ 128p^2+1,\ 256p+1,\ 256p^2+1$$

is prime.

`The case` $p = 151$. Here, $F = F_0F_1F_2F_3 = 3 \cdot 5 \cdot 17 \cdot 257$ or $F = F_1F_2F_3F_4 = 5 \cdot 17 \cdot 257 \cdot 65537$. However, this is not convenient since none of $2p+1, 2p^2+1, 4p+1, 4p^2+1$ is prime.

`The case` $p = 131$. In this case, $F = F_1F_2F_4 = 5 \cdot 17 \cdot 65537$. Now $2p+1$ is prime but $2p^2+1$ is not. So, n_1 cannot be 1. Also, neither of $4p+1,\ 4p^2+1$ is prime so n_1 cannot be 2, which is a contradiction since $\ell_1 = 2$.

`The case` $p = 127$. In this case, we have $F = F_0F_1F_2 = 3 \cdot 5 \cdot 17$ or $F = F_0F_2F_4 = 3 \cdot 17 \cdot 65537$ or $F = F_1F_2F_3 = 5 \cdot 17 \cdot 257$ or $F = F_2F_3F_4 = 17 \cdot 257 \cdot 65537$. Neither of $2p+1,\ 2p^2+1$ is prime, so the Fermat prime 3 cannot be involved. Also, $8p+1, 8p^2+1, 16p+1, 16p^2+1$ are all composite so we cannot have $n_1 \in \{3, 4\}$. However, $4p+1$ is prime and $4p^2+1$ is composite. So the only possibility is $P_1 = 4p+1$ and $F_1 = 5$ are both involved in N and 5 is the smallest Fermat prime in N. Then $257 \mid 2^n p^2 + 1$. Since the order of 2 modulo 257 is 16, we check whether $2^i p^2 + 1$ is a multiple of 257 for $i = 0, \ldots, 15$ and find no solution.

`The case` $p = 113$. The only possibility is $F = F_2F_3F_4 = 17 \cdot 257 \cdot 65537$. We have that $2p+1$ is prime but $2p^2+1$ is not, so $n_1 > 1$. Since also none of

$$4p+1,\ 4p^2+1,\ 8p+1,\ 8p^2+1,\ 16p+1,\ 16p^2+1$$

is prime, we get a contradiction.

`The case` $p = 107$. We then have $F = F_1F_3 = 5 \cdot 257$. This is not convenient since none of $2p+1, 2p^2+1, 4p+1, 4p^2+1$ is prime.

`The case` $p = 83$. We have $F = F_1F_4 = 5 \cdot 65537$. We have $2p+1$ is prime but $2p^2+1$ is not. Further, none of $4p+1, 4p^2+1$ is prime, which is a contradiction.

`The case` $p = 47$. In this case, we have $F = F_1F_4 = 5 \cdot 65537$, or $F = F_0F_1F_3 = 3 \cdot 5 \cdot 257$. We have $2p+1, 2p^2+1, 4p+1$ are all composite but $4p^2+1$ is prime. Thus, the only possibility is $n_1 = 2$ and $F = F_1F_4$ is involved in N. Thus, $65537 \mid 2^n p^2+1$. The order of 2 modulo 65537 is 32 and we check that $2^i p^2 + 1 \not\equiv 0 \pmod{65537}$ for any $i = 0, \ldots, 31$.

`The case` $p = 43$. In this case $F = F_1F_2F_3 = 5 \cdot 17 \cdot 257$, or $F = F_2F_3F_4 = 17 \cdot 257 \cdot 65537$. None of $2p+1, 2p^2+1$ is prime so $n_1 > 1$. None of

$$8p+1,\ 8p^2+1,\ 16p+1,\ 16p^2+1$$

is prime so we cannot have $n_2 \in \{3, 4\}$. However, $4p+1$ is prime (and $4p^2+1$ is not), so $n_1 = 2$, $P_1 = 4p+1$ and $F = 5 \cdot 17 \cdot 257$. Thus, $257 \mid 2^n \cdot p^2+1$. This is false as it can be checked that $2^i p^2 + 1$ is not a multiple of 257 for any $i = 0, 1, \ldots, 15$.

`The case` $p = 41$. In this case $F = F_0F_1F_3 = 3 \cdot 5 \cdot 257$. We have $2p+1$ is prime but $2p^2+1$ is not. So, $n_1 = 1$ and $257 \mid 2^n p^2 + 1$. Again we check that this is false by checking that $2^i p^2 + 1$ is not a multiple of 257 for any $i = 0, \ldots, 15$.

`The case` $p = 31$. Here, $F = F_0F_1F_2F_3 = 3 \cdot 5 \cdot 17 \cdot 257$ or $F = F_1F_2F_3F_4 = 5 \cdot 17 \cdot 257 \cdot 65537$, but none of $2p+1, 2p^2+1, 4p+1, 4p^2+1$ is prime.

`The case` $p = 29$. In this case $F = F_2F_3F_4 = 17 \cdot 257 \cdot 65537$. None of

$$2p+1,\ 2p^2+1,\ 4p+1,\ 4p^2+1$$

is prime so $n_1 \geq 3$. We have that $8p+1$ is prime but $8p^2+1$ is not so $n_1 > 3$. Finally, $16p+1$ is not prime but $16p^2+1$ is, so $n_1 = 4$ and $F = 17 \cdot 257 \cdot 65537$. We check that $65537 \mid 2^n p^2 + 1$ is impossible by checking that $2^i p^2 + 1$ is not a multiple of 65537 for any $i = 0, \ldots, 31$.

`The case` $p = 19$. In this case $F = F_0F_2F_3F_4 = 3 \cdot 17 \cdot 257 \cdot 65537$. However, this is not possible as none of $2p+1, 2p^2+1$ is prime.

`The case` $p = 13$. In this case $F = F_2F_3 = 17 \cdot 257$, or $F = F_3F_4 = 257 \cdot 65537$. We have $2p+1$ and $2p^2+1$ are composite. However, both $4p+1,\ 4p^2+1$ are primes. If $n_1 = 2$, then $P_1 = 4p+1,\ Q_1 = 4p^2+1$. Then $P_1Q_1 = (1 + 4p(p+1) + 16p^2)$ and $2 \| p+1$. So, we must have that one of $8p+1, 8p^2+1$ is involved in N, but none is a prime. Hence, $n_1 > 2$. None of

$$16p+1,\ 16p^2+1,\ 32p+1,\ 32p^2+1,\ 64p+1,\ 64p^2+1,\ 128p+1,\ 128p^2+1$$

is prime. Also, $256p^2+1$ is not prime but $256p+1$ is prime. So, we may have $n_1 = 8$, $P_1 = 256p+1$ and $F = 257 \cdot 65537$ is involved in N. Again we check that $65537 \nmid 2^n p^2 + 1$ by checking that $2^i p^2 + 1$ is never a multiple of 65537 for $i = 0, \ldots, 31$.

`The case` $p = 11$. Then $F = F_0F_3 = 3\cdot 257$, or $F = F_1F_2F_3F_4 = 5\cdot 17\cdot 257\cdot 65537$. We have that $2p+1$ is prime but $2p^2+1$ is not. So, we may have $n_1 = 1$ and then $3\cdot 257$ is involved in N. In this case, $F = 3\cdot 257$ is involved in N. Further, it follows that $F_1P_1 = (2+1)(2p+1) = (1+4p+2(p+1))$. Since $8 \mid 2(p+1)$, it follows that one of $4p+1$ or $4p^2+1$ must be a prime involved in N, but none of these is prime. Thus, $n_1 > 1$ and since none of $4p+1,\ 4p^2+1$ is prime, the number 5 cannot be involved in N, a contradiction.

`The case` $p = 7$. In this case $F = F_0F_1 = 3\cdot 5$, or $F = F_0F_3 = 3\cdot 257$, or $F = F_1F_2 = 5\cdot 17$, or $F = F_1F_4 = 5\cdot 65537$, or $F = F_2F_3 = 17\cdot 257$, or $F = F_3F_4 = 257\cdot 65537$, or $F = F_0F_1F_2F_3 = 3\cdot 5\cdot 17\cdot 257$, or $F = F_0F_1F_3F_4 = 3\cdot 5\cdot 257\cdot 65537$, or $F = F_1F_2F_3F_4 = 5\cdot 17\cdot 257\cdot 65537$. At any rate, none of $2p+1,\ 2p^2+1$ is prime so 3 is not involved in N. Now 65537 does not divide 2^np^2+1 for any n as it can be checked that 2^ip^2+1 is not a multiple of 65537 for $i = 0,\ldots,31$. Thus, 65537 is not involved in N. Similarly, 257 is not involved in N. So, the only Fermat numbers that can be involved in N are 5 and 17 and there must be at least two of them so $F = 5\cdot 17$. It thus follows that one of $4p+1,\ 4p^2+1$ is involved in N but not both (they are both prime). Assume the one involved is $4p^2+1$. Then $(4+1)\cdot(4p^2+1) = (16p^2+4(p^2+1))$ and $2\|p^2+1$. So, we need one of $8p+1,\ 8p^2+1$ to be involved in N but none is prime. Assume next that the one involved is $4p+1$. Then $(4+1)(4p+1) = (16p+4(p+1))$ and $2^7\|4(p+1)$. Since 17 is already involved in N, it follows that either both $16p+1,\ 16p^2+1$ is involved in N (false since $16p^2+1$ is not prime), or none of them is. So, none of them is. Then $5\cdot 17\cdot(4p+1) = (1+2^5m)$ for some odd m, so one of $32p+1,\ 32p^2+1$ is involved in N and this is false since they are both composite.

2.3. The Case $F = 1$

Here, $n_1 = m_1$. Let $P_1 = 2^ap+1,\ Q_1 = 2^ap^2+1$. Note that 2^mp^2+1 is a multiple of 3 if m is odd, so all m_j are even. In particular, a is even, so $p \equiv 1 \pmod 3$. This shows that all n_j are even otherwise $2^{n_j}p+1$ is a multiple of 3 for n_j odd. We can even do a bit better. Note that $p^2 \pmod 5 \in \{1,4\}$ and $a = 2a_1$ is even. So, if $p^2 \equiv 1 \pmod 4$, we cannot have a_1 odd since then $2^a \equiv 2^{2a_1} \equiv 4 \pmod 5$ so $5 \mid 2^ap^2+1$. Thus, if $p^2 \equiv 1 \pmod 5$, then $a_1 \equiv 0 \pmod 2$ and if $p^2 \equiv 4 \pmod 5$, then $a_1 \equiv 1 \pmod 2$. This also shows that $p \not\equiv 4 \pmod 5$.

Then

$$P_1Q_1 = 2^{2a}p^3 + 2^ap(p+1) + 1.$$

Assume that $\min\{n_2, m_2\} > a + \nu_2(p+1)$. Recall that $\nu_2(p+1)$ is the exponent of 2 in the factorization of $p+1$. It then follows that $a = \nu_2(p+1)$ and for this value of a both $2^ap+1,\ 2^ap^2+1$ are primes. Mathematica revealed that there are only 24 such primes p in $[7, 50000]$, namely

$$\{67, 163, 883, 3067, 3307, 6991, 7951, 13267, 14683, 16603, 17551, 18523, 22147,$$

$$23563, 24763, 27631, 28867, 37747, 38923, 40591, 43963,\ 49363, 49603, 49843\}.$$

Now we follow the proof. We need $2^n p^2 + 1$ to be a multiple of both $2^a p + 1$ and $2^a p^2 + 1$. Thus,

$$n - 2a \equiv 0 \pmod{o_1} \qquad \text{and} \qquad n - a \equiv 0 \pmod{O_1},$$

where $o_1 = \operatorname{ord}_{P_1}(2)/\gcd(2, \operatorname{ord}_{P_1}(2))$, and $O_1 = \operatorname{ord}_{Q_1}(2)$. Thus, we want that $n - 2a \equiv n - a \pmod{d}$, where $d := \gcd(o_1, O_1)$. This means $d \mid a$. A computer program ran for a few seconds and found no instance for which $d \mid a$.

Next we assume that $b = \min\{n_2, m_2\} \le a + \nu_2(p+1)$. Since $b > a$ must be even, it follows that $p \equiv 3 \pmod 4$, so $p \equiv 7 \pmod{12}$. There are 969 primes $p \in [7, 50000]$ such that $p \equiv 7 \pmod{12}$ and $p \not\equiv 4 \pmod 5$. For each one of them, we have

$$n - 2a \equiv 0 \pmod{o_1} \qquad \text{and} \qquad n - a \equiv 0 \pmod{o_2}.$$

Since $o_1 > 3a$, we get that $5a < n < 55010$ and since $a = 2a_1$, we get

$$a_1 < n/10 \qquad \text{so} \qquad a_1 \le 5000.$$

Further, $a_1 = 2a_2 + w_p$, where $w_p = 0$ if $p^2 \equiv 1 \pmod 5$ and $w_p = 1$ if $p^2 \equiv 4 \pmod 5$.

So, we wrote a code which goes through the 969 primes $p \in [7, 50000]$ satisfying $p \equiv 7 \pmod{12}$ and $p \not\equiv 4 \pmod 5$, and through all integers

$$0 \le a_2 \le 2500$$

and calculates whether with $a_1 = 2a_2 + w_p$, both numbers

$$P_1 = 2^{2a_1} p + 1 \qquad \text{and} \qquad 2^{2a_1} p^2 + 1$$

are primes. If they are, the code computes $o_1 = \operatorname{ord}_{P_1}(2)/\gcd(2, \operatorname{ord}_{P_1}(2))$ and $O_1 = \operatorname{ord}_{Q_1}(2)$, and checks whether $d = \gcd(o_1, O_1)$ divides $a = 2a_1$.

The Mathematica code ran for less than 24 hours and produced no examples. This finishes the proof.

Acknowledgement. We thank the anonymous referee for a careful reading of our paper and for suggestions that helped improve the final version of this manuscript.

References

[1] A. Alahmadi and F. Luca, There are no Carmichael numbers of the form $2^n p + 1$ with p prime, *C. R. Math.* **360** (2022), 1177–1181.

[2] J. Cilleruelo, F. Luca and A. Pizarro-Madariaga, Carmichael numbers in the sequence $(2^n k + 1)_{n\geq 1}$, *Math. Comp.* **85** (2016), 357–377.

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

[4] T. Wright, The impossibility of certain types of Carmichael numbers, *Integers* **12** (2012), 951–964.