INSTITUT DE FRANCE
Académie des sciences

Comptes Rendus
Mathématique

Adel Alahmadi and Florian Luca

There are no Carmichael numbers of the form $2^n p + 1$ with p prime

Volume 360 (2022), p. 1177-1181

https://doi.org/10.5802/crmath.393

This article is licensed under the
Creative Commons Attribution 4.0 International License.
http://creativecommons.org/licenses/by/4.0/

Les Comptes Rendus. Mathématique *sont membres du*
Centre Mersenne pour l'édition scientifique ouverte
www.centre-mersenne.org
e-ISSN : 1778-3569

Comptes Rendus
Mathématique
2022, Vol. 360, p. 1177-1181
https://doi.org/10.5802/crmath.393

Number theory / *Théorie des nombres*

There are no Carmichael numbers of the form $2^n p+1$ with p prime

Adel Alahmadi[a] **and Florian Luca**[*, b, c, d]

[a] Research Group in Algebraic Structures and its Applications, King Abdulaziz University, Jeddah, Saudi Arabia

[b] School of Maths, Wits University, 1 Jan Smuts, Braamfontein 2000, Johannesburg, South Africa

[c] Centro de Ciencias Matemáticas, UNAM, Morelia, Mexico

[d] Research Group in Algebraic Structures and Applications, King Abdulaziz University, Abdulah Sulayman, Jeddah 22254, Saudi Arabia

E-mails: analahmadi@kau.edu.sa, florian.luca@wits.ac.za

Abstract. In this paper, we prove the theorem announced in the title.

2020 Mathematics Subject Classification. 11A51.

Funding. This project was funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah under grant No. (DF-595-130-1442). The authors gratefully acknowledge DSR technical and financial support. The second author was also supported by the ANR grant JINVARIANT..

Manuscript received 29 November 2021, revised 11 March 2022, accepted 8 June 2022.

1. Introduction and main result

Primality of numbers of the form $2^n k+1$ for fixed odd k and varying n has been studied by many people due to the Proth primality theorem. There are odd numbers k such that $2^n k+1$ is never prime for any n. There are infinitely many such odd numbers k. This was proved in 1960 by Sierpiński and since then such numbers are called *Sierpiński* numbers in his honor. There are infinite arithmetic progressions of Sierpiński numbers so certainly such numbers form a subset of positive lower density of all odd integers. The odd integers k which are not Sierpiński; that is of the form $k=(p-1)/2^n$ for some prime p and nonnegative integer n, also form a subset of positive lower density of all odd integers. This was proved by Erdős and Odlyzko in [4]. In particular, there is a subset of odd integers of positive lower density such that $k2^n+1$ is a prime for at least one n. Presumably, there are odd integers k for which there are infinitely many primes of the form $2^n k+1$. This is not known but a quick application of the celebrated Maynard–Tao theorem on linear forms which are simultaneously primes gives the following.

* Corresponding author.

Theorem 1. *For each $K \geq 1$ there are infinitely many odd integers k such that $k2^n + 1$ is prime for at least K values of n. That is, the sequence $\{k2^n + 1\}_{n \geq 1}$ contains at least K primes.*

Since this statement does not seem to have appeared in the literature, we supply a quick proof of it. Let $L_i(n) = a_i n + b_i$ be distinct be linear forms in the variable n such that $a_i > 0$ and b_i are integers with $\gcd(a_i, b_i) = 1$ for $i = 1, \ldots, M$. The set of linear forms is called *admissible* if for all primes p, we have

$$\#\{0 \leq n \leq p-1 : L_1(n)L_2(n)\cdots L_M(n) \equiv 0 \pmod{p}\} < p. \tag{1}$$

For the celebrated Maynard–Tao theorem on primes in simultaneous linear forms we chose the statement of [5, Theorem 6.4].

Theorem 2 (Maynard–Tao theorem). *For any integer $K \geq 2$, let M be the smallest integer such that $M \log M > e^{8K+2}$. Then for any admissible M-tuple of linear forms $L_1(n), \ldots, L_M(n)$ there exist infinitely many positive integers n such that at least K of $L_1(n), \ldots, L_M(n)$ are primes.*

Now for the proof of Theorem 1, let K be fixed, choose M with $M \log M > e^{8K+2}$ and consider $L_i(n) = 2^{(M-1)!i}(2n+1) + 1$ for $i = 1, \ldots, M$. Since $L_1(n)\cdots L_M(n)$ is a polynomial of degree M in n the admissibility condition (1) needs to be checked only for primes $p \leq M$. Note that $L_i(n)$ is odd for all $i = 1, \ldots, M$. Further, if $p \leq M$ is odd, then $p - 1 \mid (M-1)!$ so by Fermat's Little Theorem $L_i(n) \equiv 2(n+1) \pmod{p}$ for all $i = 1, \ldots, M$. This verifies condition (1), and now Theorem 2 guarantees the existence of infinitely many k's such that at least K of $L_i(k)$ for $i = 1, \ldots, M$ are primes. For such k, the sequence $\{2^n(2k+1) + 1\}_{n \geq 1}$ contains at least K primes, and in fact, these K primes all have $n \in \{1, 2, \ldots, M!\}$.

A Carmichael number is an odd integer N which is composite but behaves like a prime with respect to the conclusion of Fermat's little theorem. Namely, $a^N \equiv a \pmod{N}$ holds for all integers a. There are infinitely many Carmichael numbers, a theorem first proved by Alford, Granville and Pomerance in 1994 in [1]. There is an easy criterion due to Korselt to check whether N is a Carmichael number. Namely, the composite positive integer N is Carmichael if and only if N is squarefree and $p - 1$ divides $N - 1$ for all prime factors p of N.

Some authors fixed an odd integer k and asked for Carmichael numbers in the sequence $\{2^n k + 1\}_{n \geq 1}$. The results are quite different from the case of primes. There are only finitely many n such that $2^n k + 1$ is Carmichael and in fact the largest such satisfies

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

where $\tau(k)$ and $\omega(k)$ are the number of divisors, and the number of prime divisors of k, respectively, and throughout this paper all logs are natural. This is the main theorem in [3]. Letting

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

the set $\mathcal{K}$ is of asymptotic density zero (see [2]). The smallest element of $\mathcal{K}$ is 27 (see [3, Theorem 2]), and a representation indicating 27 as a member of $\mathcal{K}$ is given by

$$1729 = 27 \times 2^6 + 1$$

with the Carmichael number 1729 being known as the Ramanujan taxicab number! In this paper, we revisit the set $\mathcal{K}$ and prove the following maybe somewhat unexpected theorem.

Theorem 3. *All members of $\mathcal{K}$ are composite.*

The statement of the theorem can be rephrased by saying that there is no Carmichael number of the form $2^n p + 1$ with odd p. Hence, we get the theorem announced in the title.

2. The proof

Let $\lambda(n)$ be the Carmichael function of n. It is the exponent of the multiplicative group modulo n; namely the smallest positive integer m such that if a is coprime to n, then $a^m \equiv 1 \pmod{n}$. When n is squarefree we have $\lambda(n) = \text{lcm}[p-1 : p \mid n]$. Assume by contradiction that $p \in \mathcal{K}$ for some odd prime p. By Theorem 2 in [3], we have $p \geq 29$. Let $N = 2^n p + 1$ be a Carmichael number. Since $\lambda(N) \mid N-1$, we get that all prime factors of N are of the form $2^{m_i}\delta_i + 1$ where $\delta_i \in \{1, p\}$. To fix notation, we shall assume that

$$N = \prod_{i=1}^{r} \left(2^{m_i} + 1\right) \prod_{j=1}^{s} \left(2^{n_j} p + 1\right), \tag{2}$$

where the factors $p_i = 2^{m_i} + 1$ and $q_j = 2^{n_j} p + 1$ appearing above are primes. We also assume that $m_1 < \cdots < m_r$ (if $r > 0$) and $n_1 < \cdots < n_s$ (if $s > 0$). Thus, $r + s = \omega(N) \geq 3$. It is easy to see that both $r > 0, s > 0$ must hold. Indeed, if say $r = 0$, then the only factors that appear in (2) are $2^{n_j} p + 1$ and the n_j's are distinct. Expanding and identifying the exact power of 2 dividing $N-1$, we get $n = n_1$, which is false since $2^{n_2} \mid q_2 - 1 \mid N - 1 = 2^n p$, so $n \geq n_2$. A similar contradiction is obtained if one assumes that $s = 0$. Hence, both r and s are positive and the argument based on the exponent of 2 appearing in $N-1$ shows that $n_1 = m_1$. This can also be deduced from [6, Theorem 2]. Next, we show that in fact $r \geq 2$. Indeed, if $r = 1$, we then get

$$2^n p + 1 = \left(2^{m_1} + 1\right) \prod_{j=1}^{s} \left(2^{n_j} p + 1\right),$$

which reduced modulo p gives $2^{m_1} \equiv 0 \pmod{p}$, a contradiction. We now involve some size arguments. Let again $p_i = 2^{m_i} + 1$. Then $m_i = 2^{\alpha_i}$ for some $\alpha_i \geq 0$, so $p_i = F_{\alpha_i}$ is a Fermat prime. Here, $F_\alpha = 2^{2^\alpha} + 1$. [3, Lemma 2] shows that $p_i < p^2$. Thus,

$$\prod_{i=1}^{r} p_i = \prod_{i=1}^{r} F_{\alpha_i} \leq \left(F_{\alpha_r} - 2\right) F_{\alpha_r} < p_r^2 < p^4.$$

We now look at the q's. Let $q_j = 2^{n_j} p + 1$. Then $2^{n_j} p$ and $2^n p$ are multiplicatively independent since p is odd and $n_j < n$. This condition is required in order to apply [3, Lemma 4], which in turn shows that

$$n_j < 7\sqrt{n \log p}, \tag{3}$$

assuming $n > 3\log p$, a hypothesis which we will verify later. Thus, assuming $n > 3\log p$, we get that

$$q_j < 2^{7\sqrt{n \log p}} p + 1 < 2^{7\sqrt{n} \log p + 1.5 \log p + 1}, \tag{4}$$

where we used the fact that $1/\log 2 < 1.5$. We next get an upper bound on s. From the congruences

$$2^n p \equiv -1 \left(\text{mod } q_i\right) \quad \text{and} \quad 2^{n_i} p \equiv -1 \left(\text{mod } q_i\right),$$

we get

$$2^{n-n_i} \equiv 1 \left(\text{mod } q_i\right).$$

Thus, $n - n_i$ is a multiple of $\text{ord}_{q_i}(2)$, which is the multiplicative order of 2 modulo q_i. Since $q_i - 1 = 2^{n_i} p$, we conclude that either $p \mid \text{ord}_{q_i}(2)$, or $\text{ord}_{q_i}(2) = 2^{\beta_i}$ for some $\beta_i \leq n_i$. To show that the first possibility must occur, let us assume that the second possibility occurs and get a contradiction. Since

$$2^{2^{\beta_i}} \equiv 1 \left(\text{mod } 2^{n_i} p + 1\right),$$

we get that $2^{\beta_i} > n_i \ge n_1 = m_1 = 2^{\alpha_1}$. Hence, $\beta_i \ge \alpha_1 + 1$. Further, $2^{\beta_i} \mid n - n_i$. Thus, $n_i = n - 2^{\beta_i} k_i$ for some integer k_i. But we have $p_1 = 2^{2^{\alpha_1}} + 1 \mid 2^n p + 1$. Also, $p_1 \mid 2^{2^{\alpha_1+1}} - 1 \mid 2^{2^{\beta_i}} - 1$. This shows that

$$\begin{aligned} q_i = 2^{n_i} p + 1 = 2^{n - 2^{\beta_i} k_i} p + 1 = \left(2^n p\right)\left(2^{2^{\beta_i}}\right)^{-k_i} + 1 \\ \equiv (-1) \times 1 + 1 \pmod{p_1} \quad \equiv 0 \pmod{p_1}, \end{aligned}$$

so in fact q_i is a multiple of p_1, so it cannot be a prime. So, it must be the case that $p \mid \operatorname{ord}_{q_i}(2)$, therefore $p \mid n - n_i$. Since this is true for all n_i, we conclude that $n_i \equiv n \pmod{p}$ are all in the same residue class modulo p. Since $p \mid n - n_1$ and $n - n_1$ is nonzero (otherwise $q_1 = p$, which is false), it follows that $n > p$. Since $p > 3 \log p$ holds for $p \ge 29$, we are allowed to use inequality (4). Now since all n_j satisfy estimate (3) and are in the same residue class modulo p, we get that the number of them s satisfies

$$s \le 1 + \frac{n_s}{p} \le 1 + \frac{7\sqrt{n \log p}}{p}.$$

Putting everything together and taking logarithms we get

$$\begin{aligned} n \log 2 < \log N = \log\left(\prod_{i=1}^{r} p_i\right) + \log\left(\prod_{j=1}^{s} q_j\right) \\ < \log\left(p^4\right) + \left(7\sqrt{n \log p} + 1.5 \log p + 1\right)\left(1 + \frac{7\sqrt{n \log p}}{p}\right) \log 2. \end{aligned}$$

Expanding the product in right–hand side and moving the “main term” to the left and keeping the rest in the right, we get

$$\begin{aligned} n\left(1 - \frac{49 \log p}{p}\right) \log 2 < 4 \log p \\ + \left(7\sqrt{n \log p} + 1.5 \log p + 1 + \frac{7\sqrt{n \log p}\left(1.5 \log p + 1\right)}{p}\right) \log 2. \end{aligned}$$

Assuming $p > 700$, the left-hand side exceeds $n(\log 2)/2$. Dividing across by n and using $n > p$ yields

$$\frac{\log 2}{2} < \frac{4 \log p}{p} + (\log 2)\left(7\sqrt{\frac{\log p}{p}} + \frac{1.5 \log p}{p} + \frac{1}{p} + \frac{7\sqrt{\log p}\left(1.5 \log p + 1\right)}{p^{3/2}}\right),$$

which gives $p < 1700$. Indeed the right-hand side above is a decreasing function of p (as a linear combination with positive coefficients of decreasing functions of p such as $\log p / p$ and powers of it) and when $p = 1700$ the right-hand side evaluates to $0.345705 \ldots < 0.346 < (\log 2)/2$. Hence,

$$2^{2^{\alpha_r}} + 1 = p_r < p^2 < 1700^2,$$

so $\alpha_r \le 4$. Thus, the only Fermat primes that might be involved in N are among the first 5 of them, namely F_α for $\alpha \in [0,4]$. Further, $\lambda(N) = 2^u p$ for some $u \in [1,n]$. Main Theorem 2 in [6] then gives that N is one of the numbers

$$\begin{aligned} &5\times 13\times 17,\\ &5\times 13\times 193\times 257,\\ &5\times 13\times 193\times 257\times 769,\\ &3\times 11\times 17,\\ &5\times 17\times 29,\\ &5\times 17\times 29\times 113,\\ &5\times 29\times 113\times 65537\times 114689,\\ &5\times 17\times 257\times 509,\end{aligned}$$

but none of them is of the form $2^n p+1$ for some prime p. This finishes the argument.

3. Comments

There are a few examples of Carmichael numbers N of the form $N = 2^n p^b + 1$ for some odd prime p and positive exponent $b > 1$ such as

$$2^6\times 3^3+1,\quad 2^6\times 3^6+1.$$

Is it true that there are only finitely many Carmichael numbers of this form? If so, we would then get that $\omega(N-1) \ge 3$ holds for all Carmichael numbers N except for finitely many. Are there infinitely many Carmichael numbers N such that $\omega(N-1) = 3$? How about $\omega(N-1) = 4$? Or maybe $\omega(N-1)$ tends to infinity as N goes to infinity through Carmichael numbers? We leave such questions for future projects and maybe for future researchers.

Acknowledgements

We thank the referee for constructive comments which improved the quality of our article.

References

[1] W. R. Alford, A. Granville, C. Pomerance, "There are infinitely many Carmichael numbers", *Ann. Math.* **139** (1994), no. 3, p. 703-722.

[2] W. D. Banks, C. Finch, F. Luca, C. Pomerance, P. Stănică, "Sierpiński and Carmichael numbers", *Trans. Am. Math. Soc.* **367** (2015), no. 1, p. 355-376.

[3] J. Cilleruelo, F. Luca, A. Pizarro, "Carmichael numbers in the sequence $(2^n k+1)_{n\ge 1}$", *Math. Comput.* **85** (2016), no. 297, p. 357-377.

[4] P. Erdős, A. M. Odlyzko, "On the density of odd integers of the form $(p-1)2^{-n}$ and related questions", *J. Number Theory* **11** (1979), p. 257-263.

[5] A. Granville, "Primes in intervals of bounded length", *Bull. Am. Math. Soc.* **52** (2015), no. 2, p. 171-222.

[6] T. Wright, "The impossibility of certain types of Carmichael numbers", *Integers* **12** (2012), no. 5, p. 951-964.