PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 140, Number 1, January 2012, Pages 129–134
S 0002-9939(2011)10899-2
Article electronically published on May 20, 2011

CULLEN NUMBERS WITH THE LEHMER PROPERTY

JOSÉ MARÍA GRAU RIBAS AND FLORIAN LUCA

(Communicated by Matthew A. Papanikolas)

Abstract. Here, we show that there is no positive integer n such that the nth Cullen number $C_n = n2^n + 1$ has the property that it is composite but $\phi(C_n) \mid C_n - 1$.

1. Introduction

A *Cullen number* is a number of the form $C_n = n2^n + 1$ for some $n \geq 1$. They attracted the attention of researchers since it seems that it is hard to find primes of this form. Indeed, Hooley [8] showed that for most n the number C_n is composite. For more about testing C_n for primality, see [3] and [6]. For an integer $a > 1$, a *pseudoprime* to base a is a composite positive integer m such that $a^m \equiv a \pmod{m}$. Pseudoprime Cullen numbers have also been studied. For example, in [12], it is shown that for most n, C_n is not a base a pseudoprime. Some computer searches up to several millions did not turn up any pseudoprime C_n to any base. Thus, it would seem that Cullen numbers which are pseudoprimes are very scarce. A *Carmichael number* is a positive integer m which is a base a pseudoprime for any a. A composite integer m is called a *Lehmer number* if $\phi(m) \mid m - 1$, where $\phi(m)$ is the Euler function of m. Lehmer numbers are Carmichael numbers, hence, pseudoprimes in every base. No Lehmer number is known, although it is known that there are no Lehmer numbers in certain sequences, such as the Fibonacci sequence (see [9]), or the sequence of repunits in base g for any $g \in [2, 1000]$ (see [4]). For other results on Lehmer numbers, see [1], [2], [11], [13], [14].

Our result here is that there is no Cullen number with the Lehmer property. Hence, if $\phi(C_n) \mid C_n - 1$, then C_n is prime.

Theorem 1. *Let C_n be the nth Cullen number. If $\phi(C_n) \mid C_n - 1$, then C_n is prime.*

2. Proof of Theorem 1

Assume that $n \geq 30$, that $\phi(C_n) \mid C_n - 1$, but that C_n is not prime. Then C_n is square-free. Write

$$C_n = \prod_{i=1}^{k} p_i.$$

Received by the editors October 14, 2010 and, in revised form, November 11, 2010.
2010 *Mathematics Subject Classification.* Primary 11A05; Secondary 11N25, 11A07.

So,

$$\prod_{i=1}^{k}(p_i-1) \mid n2^n.$$

Write $n = 2^\alpha n_1$, where n_1 is odd. Then $C_n = n_1 2^{n_2} + 1$, where $n_2 := \alpha + n$. Let p be any prime factor of C_n. Since $p - 1 \mid C_n - 1$, it follows that $p = m_p 2^{n_p} + 1$ for some odd divisor m_p of n and some n_p with

$$n_p \le n_2 = n + \alpha \le n + \frac{\log n}{\log 2}.$$

Let us first show that in fact $n_p \le n$. Assume that $n_p > n$. Then,

$$C_n = n2^n + 1 = p\lambda, \tag{1}$$

for some positive integer λ, where $p \ge 2^{n+1} + 1$. Observe that $\lambda > 1$ because C_n is not prime. Now

$$\lambda = \frac{C_n}{p} \le \frac{n2^n + 1}{2^{n+1} + 1} < n.$$

Reducing equation (1) modulo 2^n, we get that $2^n \mid \lambda - 1$, so $2^n \le \lambda - 1 < n$, which is false for any $n > 1$. Hence, $n_p \le n$.

Next we look at m_p. If $m_p = 1$, then $p = 2^{n_p} + 1$ is a Fermat prime. Hence, $n_p = 2^{\gamma_p}$ for some nonnegative integer γ. Since $2^{\gamma_p} = n_p \le n$, we get that $\gamma_p < (\log n)/(\log 2)$. Hence, the prime p can take at most $1+(\log n)/(\log 2)$ values. Next, observe that since

$$\prod_{p \mid C_n} m_p \mid n, \tag{2}$$

it follows that the number of prime factors p of C_n such that $m_p > 1$ is $\le (\log n)/(\log 3)$. Hence, we have arrived at the bound

$$k < 1 + \frac{\log n}{\log 2} + \frac{\log n}{\log 3} < 1 + 2.4 \log n. \tag{3}$$

We next bound n_p. Put $N := \lfloor \sqrt{n/\log n} \rfloor$, and consider pairs (a, b) of integers in $\{0, 1, \ldots, N\}$. There are $(N + 1)^2 > n/\log n$ such pairs. For each such pair, consider the expression $L(a, b) := an + bn_p \in [0, 2n^{3/2}/(\log n)^{1/2}]$. Thus, there exist two pairs $(a, b) \ne (a_1, b_1)$ such that

$$|(a - a_1)n + (b - b_1)n_p| = |L(a, b) - L(a_1, b_1)| \le \frac{2n^{3/2}/(\log n)^{1/2}}{n/\log n - 1} < 3(n \log n)^{1/2}.$$

Put $u := a - a_1,\ v := b - b_1$. Then $(u, v) \ne (0, 0)$ and

$$|un + vn_p| < 3(n \log n)^{1/2}.$$

We may also assume that u and v are coprime, for if not, we replace the pair (u, v) by the pair (u_1, v_1), where $d := \gcd(u, v),\ u_1 := u/d,\ v_1 := v/d$, and the properties that $\max\{|u_1|, |v_1|\} \le (n/\log n)^{1/2}$ and $|u_1 n + v_1 n_p| < 3(n \log n)^{1/2}$ are still fulfilled. Finally, up to replacing the pair (u, v) by the pair $(-u, -v)$, we may assume that $u \ge 0$.

Now consider the congruences $n2^n \equiv -1 \pmod p$ and $m_p 2^{n_p} \equiv -1 \pmod p$. Observe that $2,\ n,\ m_p$ are all three coprime to p. Raise the first congruence to u and the second to v and multiply them to get

$$n^u m_p^v 2^{nu+n_p v} \equiv (-1)^{u+v} \pmod p.$$

Hence, p divides the numerator of the rational number

$$A := n^u m_p^v 2^{nu+n_p v} - (-1)^{u+v}. \tag{4}$$

Let us show that $A \neq 0$. Assume that $A = 0$. Recall that $n = 2^\alpha n_1$. Thus, expression (4) is

$$A = n_1^u m_p^v 2^{(n+\alpha)u+n_p v} - (-1)^{u+v} = 0.$$

Then $n_1^u m_p^v = 1$, $(n+\alpha)u + vn_p = 0$, and $u+v$ is even. Since $u \geq 0$, it follows that $v \leq 0$. Put $w := -v$, so $w \geq 0$. There exists an odd positive integer ρ such that $n_1 = \rho^w$ and $m_p = \rho^u$. Since u and v are coprime and $u+v$ is even, it follows that u and v are both odd. Hence, w is also odd. Also, since m_p divides n_1, it follows that $u \leq w$. We now get

$$(2^\alpha \rho^w + \alpha)u - wn_p = 0,$$

so

$$\frac{u}{n_p} = \frac{w}{2^\alpha \rho^w + \alpha}.$$

The left-hand side is $\geq u/n = u/(2^\alpha \rho^u)$, because $n_p \leq n = 2^\alpha \rho^u$. Hence, we get that

$$\frac{u}{2^\alpha \rho^u} \leq \frac{u}{n_p} = \frac{w}{2^\alpha \rho^w + \alpha} \qquad \text{leading to} \qquad \frac{u}{\rho^u} \leq \frac{w}{\rho^w + (\alpha/2^\alpha)} \leq \frac{w}{\rho^w}.$$

For $\rho \geq 3$, the function $s \mapsto s/\rho^s$ is decreasing for $s \geq 0$, so the above inequality together with the fact that $u \leq w$ implies that $u = w$ (so both are 1 because they are coprime), and that all the intermediary inequalities are also equalities. This means that $u = w = 1$, $\alpha = 0$ and $n = n_p$, but all this is possible only when $C_n = p$, which is not allowed. If $\rho = 1$, we then get that $n_1 = 1$, so every prime factor p of C_n is a Fermat prime. Hence, we get

$$C_n = 2^{n_2} + 1 = \prod_{i=1}^{k} (2^{2^{\gamma_{p_i}}} + 1) = \sum_{I \subseteq \{1,\ldots,k\}} 2^{\sum_{i \in I} 2^{\gamma_{p_i}}},$$

and $k \geq 2$, but this is impossible by the unicity of the binary expansion of C_n.

Thus, it is not possible for the expression A shown at (4) to be zero.

The size of the numerator of A is at most

$$\begin{aligned} 2^{1+|nu+n_p v|} n^u m_p^{|v|} &\leq 2^{1+3(n\log n)^{1/2}} n^{2(n/\log n)^{1/2}} \\ &< 2^{1+3(n\log n)^{1/2}+(2/\log 2)(n\log n)^{1/2}} < 2^{6(n\log n)^{1/2}}. \end{aligned}$$

In the above chain of inequalities, we used the fact that $3 + 2/\log 2 < 5.9$, together with the fact that $(n\log n)^{1/2} > 10$ for $n \geq 30$. Thus, for $n \geq 30$, we have that the inequality

$$p < 2^{6(n\log n)^{1/2}} \tag{5}$$

holds for all prime factors p of C_n.

Thus, we get the inequality

$$2^n < C_n = \prod_{i=1}^{k} p_i < \prod_{i=1}^{k} 2^{6(n\log n)^{1/2}} = 2^{6k(n\log n)^{1/2}},$$

leading to

$$k > \frac{n^{1/2}}{6(\log n)^{1/2}}. \tag{6}$$

Comparing estimates (3) and (6), we get

$$\frac{n^{1/2}}{6(\log n)^{1/2}} < 1 + 2.4\log n,$$

implying that $n < 6 \times 10^5$.

It remains to lower this bound. We first lower it to $n < 93000$. Indeed, first note that since $n < 6 \times 10^5$, it follows that if $p = F_\gamma = 2^{2^\gamma} + 1$ is a Fermat prime dividing C_n, then $\gamma \le 18$. The only such Fermat primes are for $\gamma \in \{0, 1, 2, 3, 4\}$. Furthermore, $(\log n)/(\log 3) \le \log(6 \times 10^5)/(\log 3) = 12.1104\ldots$. Hence, $k \le 5 + 12 = 17$. It then follows, by equation (6), that

$$\frac{n^{1/2}}{6(\log n)^{1/2}} < 17,$$

so $n < 122000$. But then $(\log n)/(\log 3) < \log(122000)/(\log 3) = 10.6605\ldots$, giving that in fact $k \le 15$. Inequality (6) shows that

$$\frac{n^{1/2}}{6(\log n)^{1/2}} < 15,$$

so $n < 93000$. Next let us observe that if n is not a multiple of 3, then relation (2) leads easily to the conclusion that the number of prime factors p of C_n with $m_p > 1$ is in fact $\le (\log n)/(\log 5) = 7.15338\ldots$. Hence, the number of such primes is ≤ 7, giving that $k \le 12$, which contradicts a result of Cohen and Hagis [5] who showed that every number with the Lehmer property must have at least 14 distinct prime factors. Hence, $3 \mid n$, which shows that C_n is not a multiple of 3. An argument similar to one used before proves that n is not a multiple of any prime $q > 3$. Indeed, if it were, then relation (2) would lead to the conclusion that the number of prime factors p of C_n with $m_p > 1$ is $\le 1 + \log(n/q)/(\log 3) \le 1 + \log(93000/5)/(\log 3) = 9.94849\ldots$, so there are at most 9 such primes. Also, C_n can be divisible with at most 4 of the 5 Fermat primes F_γ with $\gamma \in \{0, 1, 2, 3, 4\}$, because $3 = F_0$ does not divide C_n. Hence, $k \le 9 + 4 = 13$, which again contradicts the result from [5]. Thus, $n = 2^\alpha 3^\beta$ and so all prime factors p of C_n are of the form $2^{\alpha_1}3^{\beta_1} + 1$ for some nonnegative integers α_1 and β_1. Now write

$$a = \frac{C_n - 1}{\phi(C_n)} = \prod_{i=1}^{k}\left(1 + \frac{1}{p_i - 1}\right) \tag{7}$$

for some integer $a \ge 2$. Since

$$\prod_{\substack{\alpha_1 \ge 0,\ \beta_1 \ge 0 \\ 2^{\alpha_1}3^{\beta_1}+1 \text{ prime}}} \left(1 + \frac{1}{2^{\alpha_1}3^{\beta_1}}\right) < 1.46,$$

we get that $a < 2$, which is a contradiction. This shows that in fact there are no numbers C_n with the claimed property.

We end with some challenges for the reader.

Research problem. *Prove that C_n is not a Carmichael number for any $n \geq 1$.*

If this is too hard, can one at least give a sharp upper bound on the counting function of the set $\mathcal{C}$ of positive integers n such that C_n is a Carmichael number? We recall that Heppner [7] proved that if x is large, then the number of positive integers $n \leq x$ such that C_n is prime is $O(x/\log x)$, whereas in [12] it was shown that if $a > 1$ is a fixed integer, then the number of positive integers $n \leq x$ such that C_n is base a pseudoprime is $O(x(\log\log x)/\log x)$. Clearly, imposing that C_n is Carmichael (which is a stronger condition) should lead to sharper upper bounds for the counting function of such indices n.

Finally, here is a problem suggested to us by the referee. Theorem 1 shows that $\phi(C_n)/\gcd(C_n - 1, \phi(C_n))$ exceeds 1 for all n. Can one say something more about this ratio? For example, it is possible that a minor modification of the arguments in the paper would show that this function tends to infinity with n, but we have not worked out the details of such a deduction. It would be interesting to find a good (large) lower bound on this quantity which is valid for all n and which tends to infinity with n. How about for most n? What about lower and upper bounds on the average value of this function when n ranges in the interval $[1, x]$ and x is a large real number? We leave these questions for further research.

Acknowledgements

We thank the referee for a careful reading of the paper and for suggesting some of the questions mentioned at the end. The second author was supported in part by grants PAPIIT 100508 and SEP-CONACyT 79685.

References

[1] W. D. Banks, A. M. Güloğlu and C. W. Nevans, 'On the congruence $N \equiv A \pmod{\varphi(N)}$', *Integers* **8** (2008), #A59. MR2472077 (2010g:11154)

[2] W. D. Banks and F. Luca, 'Composite integers n for which $\varphi(n) \mid n-1$', *Acta Math. Sinica* **23** (2007), 1915–1918. MR2352307 (2008j:11134)

[3] P. Berrizbeitia and J. G. Fernandes, 'Observaciones sobre la primalidad de los números de Cullen', short communication in "Terceras Jornadas de Teoría de Números" (http://campus.usal.es/∼tjtn2009/doc/abstracts.pdf).

[4] J. Cilleruelo and F. Luca, 'Repunit Lehmer numbers', *Proc. Edinburgh Math. Soc.* **54** (2011), 55–65.

[5] G. L. Cohen and P. Hagis, 'On the number of prime factors of n if $\phi(n) \mid n - 1$', *Nieuw Arch. Wisk.* **28** (1980), 177–185. MR582925 (81j:10002)

[6] J. M. Grau and A. M. Oller-Marcén, 'An $\widetilde{O}(\log^2 N)$ time primality test for generalized Cullen numbers', preprint, 2010, to appear in *Math. Comp.*

[7] F. Heppner, 'Über Primzahlen der Form $n2^n + 1$ bzw. $p2^p + 1$', *Monatsh. Math.* **85** (1978), 99–103. MR0567136 (58:27859)

[8] C. Hooley, *Applications of sieve methods to the theory of numbers*, Cambridge University Press, Cambridge, 1976. MR0404173 (53:7976)

[9] F. Luca, 'Fibonacci numbers with the Lehmer property', *Bull. Pol. Acad. Sci. Math.* **55** (2007), 7–15. MR2304295 (2008g:11024)

[10] F. Luca, 'On the greatest common divisor of two Cullen numbers', *Abh. Math. Sem. Univ. Hamburg* **73** (2003), 253–270. MR2028519 (2004i:11001)

[11] F. Luca and C. Pomerance, 'On composite integers n for which $\phi(n) \mid n - 1$', *Bol. Soc. Mat. Mexicana*, to appear.

[12] F. Luca and I. E. Shparlinski, 'Pseudoprime Cullen and Woodall numbers', *Colloq. Math.* **107** (2007), 35–43. MR2283130 (2007i:11127)
[13] C. Pomerance, 'On the distribution of amicable numbers', *J. reine angew. Math.* **293/294** (1977), 217–222. MR0447087 (56:5402)
[14] C. Pomerance, 'On composite n for which $\varphi(n) \mid n-1$, II', *Pacific J. Math.* **69** (1977), 177–186. MR0434938 (55:7901)

Departamento de Mátematicas, Universidad de Oviedo, Avenida Calvo Sotelo, s/n, 33007 Oviedo, Spain
E-mail address: grau@uniovi.es

Instituto de Matemáticas, Universidad Nacional Autonoma de México, C.P. 58089, Morelia, Michoacán, México
E-mail address: fluca@matmor.unam.mx