LUCAS NUMBERS WITH THE LEHMER PROPERTY

BERNADETTE FAYE and FLORIAN LUCA

Communicated by Vasile Brînzănescu

A composite positive integer n is *Lehmer* if $\phi(n)$ divides $n-1$, where $\phi(n)$ is the Euler's totient function. No Lehmer number is known, nor has it been proved that they don't exist. In 2007, the second author [7] proved that there is no Lehmer number in the Fibonacci sequence. In this paper, we adapt the method from [7] to show that there is no Lehmer number in the companion Lucas sequence of the Fibonacci sequence $(L_n)_{n\geq 0}$ given by $L_0 = 2, L_1 = 1$ and $L_{n+2} = L_{n+1} + L_n$ for all $n \geq 0$.

AMS 2010 Subject Classification: 11B39, 11A25.

Key words: Lucas numbers, Euler function.

1. INTRODUCTION

Let $\phi(n)$ be the Euler function of a positive integer n. Recall that if n has the prime factorization

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

then

$$\phi(n) = (p_1 - 1)p_1^{\alpha_1 - 1}(p_2 - 1)p_2^{\alpha_2 - 1} \cdots (p_k - 1)p_k^{\alpha_k - 1}.$$

Lehmer [6] conjectured that if $\phi(n) \mid n-1$ then n is a prime. To this day, the conjecture remains open. Counterexamples to Lehmer's conjecture have been dubbed *Lehmer numbers*. Several people worked on getting larger and larger lower bounds on a potential Lehmer number. For a positive integer m, we write $\omega(m)$ for the number of distinct prime factors of m. Lehmer himself proved that if N is Lehmer, then $\omega(N) \geq 7$. This has been improved by Cohen and Hagis [3] to $\omega(N) \geq 14$. The current record $\omega(N) \geq 15$ is due to Renze [9]. If additionally $3 \mid N$, then $\omega(N) \geq 40 \cdot 10^6$ and $N > 10^{36 \cdot 10^7}$.

Not succeeding in proving that there are no Lehmer numbers, some researchers have settled for the more modest goal of proving that there are no Lehmer numbers in certain interesting subsequences of positive integers. For example, in [7], Luca proved that there is no Fibonacci number which is Lehmer. In [5], it is shown that there is no Lehmer number in the sequence of Cullen numbers $\{C_n\}_{n\geq 1}$ of general term $C_n = n2^n + 1$, while in [4] the same conclusion is shown to hold for generalized Cullen numbers. In [2], it is shown that there is no Lehmer number of the form $(g^n - 1)/(g - 1)$ for any $n \geq 1$ and integer $g \in [2, 1000]$.

Here, we apply the same argument as in [7], to the Lucas sequence companion of the Fibonacci sequence given by $L_0 = 2, L_1 = 1$ and $L_{n+2} = L_{n+1} + L_n$ for all $n \geq 0$. Putting $(\alpha, \beta) = ((1 + \sqrt{5})/2, (1 - \sqrt{5})/2)$ for the two roots of the characteristic equation $x^2 - x - 1 = 0$ of the Lucas sequence, the Binet formula

$$L_n = \alpha^n + \beta^n \qquad \text{holds for all} \qquad n \geq 0. \tag{1}$$

There are several relations among Fibonacci and Lucas numbers which are well-known and can be proved using the Binet formula (1) for the Lucas numbers and its analog

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \qquad \text{for all} \qquad n \geq 0$$

for the Fibonacci numbers. Some of them which are useful for us are

$$L_n^2 - 5F_n^2 = 4(-1)^n, \tag{2}$$

$$L_n = L_{n/2}^2 - 2(-1)^{n/2} \quad \text{valid for all even} \quad n, \tag{3}$$

whereas for odd n

$$L_n - 1 = \begin{cases} 5F_{(n+1)/2}F_{(n-1)/2} & \text{if} \quad n \equiv 1 \pmod 4; \\ L_{(n+1)/2}L_{(n-1)/2} & \text{if} \quad n \equiv 3 \pmod 4). \end{cases} \tag{4}$$

Our result is the following:

Theorem 1. *There is no Lehmer number in the Lucas sequence.*

2. PROOF

Assume that L_n is Lehmer for some n. Clearly, L_n is odd and $\omega(L_n) \geq 15$ by the main result from [9]. The product of the first 15 odd primes exceeds 1.6×10^{19}, so $n \geq 92$. Furthermore,

$$2^{15} \mid 2^{\omega(L_n)} \mid \phi(L_n) \mid L_n - 1. \tag{5}$$

If n is even, formula (3) shows that $L_n - 1 = L_{n/2}^2 + 1$ or $L_{n/2}^2 - 3$ and numbers of the form $m^2 + 1$ or $m^2 - 3$ for some integer m are never multiples of 4, so divisibility (5) is impossible. If $n \equiv 3 \pmod 8$, relations (4) and (5) show that $2^{15} \mid L_{(n+1)/2}L_{(n-1)/2}$. This is also impossible since no member of the Lucas sequence is a multiple of 8, fact which can be easily proved by listing its first 14 members modulo 8:

$$2,\ 1,\ 3,\ 4,\ 7,\ 3,\ 2,\ 5,\ 7,\ 4,\ 3,\ 7,\ 2,\ 1,$$

and noting that we have already covered the full period of $\{L_m\}_{m\ge 0}$ modulo 8 (of length 12) without having reached any zero.

So, we are left with the case when $n \equiv 1 \pmod 4$.

Let us write

$$n = p_1^{\alpha_1}\cdots p_k^{\alpha_k},$$

with $p_1 < \cdots < p_k$ odd primes and $\alpha_1, \ldots, \alpha_k$ positive integers. If $p_1 = 3$, then L_n is even, which is not the case. Thus, $p_1 \ge 5$.

Here, we use the argument from [7] to bound p_1. Since most of the details are similar, we only sketch the argument. Let p be any prime factor of L_n. Reducing formula (1) modulo p we get that $-5F_n^2 \equiv -4 \pmod p$. In particular, 5 is a quadratic residue modulo p, so by Quadratic Reciprocity also p is a quadratic residue modulo 5. Now let d be any divisor of n which is a multiple of p_1. By Carmichael's Primitive Divisor Theorem for the Lucas numbers (see [1]), there exists a primitive prime $p_d \mid L_d$, such that $p_d \nmid L_{d_1}$ for all positive $d_1 < d$. Since n is odd and $d \mid n$, we have $L_d \mid L_n$, therefore $p_d \mid L_n$. Since p_d is primitive for L_d and a quadratic residue modulo 5, we have $p_d \equiv 1 \pmod d$ (if p were not a quadratic residue modulo 5, then we would have had that $p_d \equiv -1 \pmod 5$, which is less useful for our problem). In particular,

$$p_1 \mid d \mid p_d - 1 \mid \phi(L_n). \tag{6}$$

Collecting the above divisibilities (6) over all divisors d of n which are multiples of p_1 and using (4), we have

$$p_1^{\tau(n/p_1)} \mid \phi(L_n) \mid L_n - 1 \mid 5F_{(n-1)/2}F_{(n+1)/2}. \tag{7}$$

In the above, $\tau(m)$ is the number of divisors of m. If $p_1 = 5$, then $5 \mid n$, therefore $5 \nmid F_{(n\pm1)/2}$ because a Fibonacci number F_m is a multiple of 5 if and only if its index m is a multiple of 5. Thus, $\tau(n/p_1) = 1$, so $n = p_1$, which is impossible since $n > 92$.

Assume now that $p_1 > 5$. Since

$$\gcd(F_{(n+1)/2}, F_{(n-1)/2}) = F_{\gcd((n+1)/2,(n-1)/2)} = F_1 = 1,$$

divisibility relation (7) shows that $p_1^{\tau(n/p_1)}$ divides $F_{(n+\varepsilon)/2}$ for some $\varepsilon \in \{\pm 1\}$. Let $z(p_1)$ be the order of appearance of p_1 in the Fibonacci sequence, which is the minimal positive integer ℓ such that $p_1 \mid F_\ell$. Write

$$F_{z(p_1)} = p_1^{e_{p_1}} m_{p_1}, \tag{8}$$

where m_{p_1} is coprime to p_1. It is known that $p_1 \mid F_k$ if and only if $z(p_1) \mid k$. Furthermore, if $p_1^t \mid F_k$ for some $t > e_{p_1}$, then necessarily $p_1 \mid k$. Since for us $(n+\varepsilon)/2$ is not a multiple of p_1 (because n is a multiple of p_1), we get that $\tau(n/p_1) \le e_{p_1}$. In particular, if $p_1 = 7$, then $e_{p_1} = 1$, so $n = p_1$, which is false since $n > 92$. So, $p_1 \ge 11$. We now follow along the argument from [7] to get that

$$\tau(n) \le 2\tau(n/p_1) \le \frac{(p_1+1)\log\alpha}{\log p_1}. \tag{9}$$

Further, since $(L_n - 1)/\phi(L_n)$ is an integer larger than 1, we have

$$2 < \frac{L_n}{\phi(L_n)} \le \prod_{p \mid L_n}\left(1 + \frac{1}{p-1}\right) < \exp\left(\sum_{p \mid L_n} \frac{1}{p-1}\right), \tag{10}$$

or

$$\log 2 \le \sum_{p \mid L_n} \frac{1}{p-1}. \tag{11}$$

Letting for a divisor d of n the notation $\mathcal{P}_d$ stand for the set of primitive prime factors of L_d, the argument from [7] gives

$$\sum_{p \in \mathcal{P}_d} \frac{1}{p-1} \le \frac{0.9}{d} + \frac{2.2\log\log d}{d}. \tag{12}$$

Since the function $x \mapsto (\log\log x)/x$ is decreasing for $x > 10$ and all divisors $d > 1$ of n satisfy $d > 10$, we have, using (9), that

$$\begin{aligned} \sum_{p \mid L_n} \frac{1}{p-1} &= \sum_{d \mid n} \sum_{p \in \mathcal{P}_d} \frac{1}{p-1} \le \sum_{\substack{d \mid n \\ d > 1}} \left(\frac{0.9}{d} + \frac{2.2\log\log d}{d}\right) \\ &\le \left(\frac{0.9}{p_1} + \frac{2.2\log\log p_1}{p_1}\right)\tau(n) \\ &\le (\log\alpha)\frac{(p_1+1)}{\log p_1} \cdot \left(\frac{0.9}{p_1} + \frac{2.2\log\log p_1}{p_1}\right), \end{aligned} \tag{13}$$

which together with inequality (11) leads to

$$\log p_1 \le \frac{(\log\alpha)}{\log 2}\left(\frac{p_1+1}{p_1}\right)(0.9 + 2.2\log\log p_1). \tag{14}$$

The above inequality (14) implies $p_1 < 1800$. Since $p_1 < 10^{14}$, a calculation of McIntosh and Roettger [8] shows that $e_{p_1} = 1$. Thus, $\tau(n/p_1) = 1$, therefore $n = p_1$. Since $n \ge 92$, we have $p_1 \ge 97$. Going back to the inequalities (11) and (12), we get

$$\log 2 < \frac{0.9}{p_1} + \frac{2.2 \log\log p_1}{p_1},$$

which is false for $p_1 \geq 97$. The theorem is proved.

Acknowledgments. B.F. thanks OWSD and Sida (Swedish International Development Cooperation Agency) for a scholarship during her Ph.D. studies at Wits.

REFERENCES

[1] R.D. Carmichael, *On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$.* Ann. of Math. (2) **15** (1913), 30-70.

[2] J. Cilleruelo and F. Luca, *Repunit Lehmer numbers.* Proc. Edinb. Math. Soc. (2) **54** (2011), *1*, 55–65.

[3] G.L. Cohen and P. Hagis, *On the number of prime factors of n if $\phi(n) \mid n-1$.* Nieuw Arch. Wiskd. **28** (1980), *3*, 177–185.

[4] D.-J. Kim and B.-K. Oh, *Generalized Cullen numbers with the Lehmer Property.* Bull. Korean Math. Soc. **50** (2013), *6*, 1981–1988.

[5] J.M. Grau Ribas and F. Luca, *Cullen numbers with the Lehmer property.* Proc. Amer. Math. Soc. **140** (2012),*1*, 129–134.

[6] D.H. Lehmer, *On Euler totient function.* Bull. Amer. Math. Soc. **38** (1932), 745–751.

[7] F. Luca, *Fibonacci numbers with the Lehmer property.* Bull. Pol. Acad. Sci. Math. **55** (2007), *1*, 7–15.

[8] R.J. McIntosh and E.L. Roettger, *A search for Fibonacci Wiefrich and Wolsenholme primes.* Math. Comp. **76** (2007), *260*, 2087–2094.

[9] J. Renze, *Computational evidence for Lehmer's totient conjecture.* Published electronically at http://library.wolfram.com/ infocenter/MathSource/5483/, 2004.

[10] D.D. Wall, *Fibonacci series modulo m.* Amer. Math. Monthly **67** (1960), 525–532.

Received 24 July 2015

Université Cheikh Anta Diop de Dakar,
Ecole Doctorale de Mathematiques
et d'Informatique,
BP 5005, Dakar Fann, Senegal
University of the Witwatersrand,
School of Mathematics,
Private Bag X3, Wits 2050,
Johannesburg, South Africa
bernadette@aims-senegal.org

University of the Witwatersrand,
School of Mathematics,
Private Bag X3, Wits 2050,
Johannesburg, South Africa
Florian.Luca@wits.ac.za