ON FIBONACCI NUMBERS WHICH ARE ELLIPTIC KORSELT NUMBERS

FLORIAN LUCA AND PANTELIMON STĂNICĂ

ABSTRACT. Here, we show that if E is a CM elliptic curve with CM field $\mathbb{Q}(\sqrt{-d})$, then the set of n for which the nth Fibonacci number F_n satisfies an elliptic Korselt criterion for $\mathbb{Q}(\sqrt{-d})$ (defined in the paper) is of asymptotic density zero.

1. INTRODUCTION

Let $b \geq 2$ be an integer. A composite integer n is a pseudoprime to base b if the congruence $b^n \equiv b \pmod{n}$ holds. There are infinitely many pseudoprimes with respect to any base b, but they are less numerous than the primes. That is, putting $\pi_b(x)$ for the number of base b pseudoprimes $n \leq x$, a result of Pomerance [9] shows that the inequality

$$\pi_b(x) \leq x/L(x)^{1/2} \qquad \text{where} \qquad L(X) = \exp\left(\log x \log\log\log x / \log\log x\right)$$

holds for all sufficiently large x. It is conjectured that $\pi_b(x) = x/L(x)^{1+o(1)}$ as $x \to \infty$.

Let $\{F_n\}_{n\geq 0}$ be the sequence of Fibonacci numbers $F_{n+1} = F_n + F_{n-1}$ for $n \geq 1$ with $F_0 = 0, F_1 = 1$, and $\{L_n\}_{n\geq 0}$ be its companion Lucas sequence satisfying the same recurrence with initial conditions, $L_0 = 2, L_1 = 1$. For the Fibonacci sequence $\{F_n\}_{n\geq 1}$ is was shown in [7] that the set of $n \leq x$ such that F_n is a prime or a base b pseudoprime is of asymptotic density zero. More precisely, it was shown that the number of such $n \leq x$ is at most $5x/\log x$ if x is sufficiently large.

Since elliptic curves have become very important in factoring and primality testing, several authors have defined and proved many results on elliptic pseudoprimes. To define an elliptic pseudoprime, let E be an elliptic curve over $\mathbb{Q}$ with complex multiplication by $\mathbb{Q}(\sqrt{-d})$. Here, $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$. If p is a prime not dividing $6\Delta_E$, where Δ_E is the discriminant of E, and additionally $(-d|p) = -1$, where $(a|p)$ denotes the Legendre symbol of a with respect to p, then the order of the group of points on E modulo p denoted $\#E(\mathbb{F}_p)$, equals $p+1$. In case $p \nmid \Delta_E$ and $(-d|p) = 1$, we have $\#E(\mathbb{F}_p) = p + 1 - a_p$ for some nonzero integer a_p with $|a_p| < 2\sqrt{p}$. Gordon [3], used the simple formula for $\#\mathbb{E}(\mathbb{F}_p)$ in the case $(-d|p) = -1$ to define the following test of compositeness: Let Q be a point in $E(\mathbb{Q})$ of infinite order. Let $N > 163$ be a number coprime to 6 to be tested. We compute $(-d|N)$. If it is 1 we do not test and if it is 0, then N is composite. If it is -1, then we compute $[N+1]Q \pmod{N}$. If it is not O (the identity element of $E(\mathbb{Q})$), then N is composite while if it is O, then we declare N to be a probable prime for $Q \in E$. So, we can define N to be a pseudoprime for $Q \in E$ if it is composite and probable prime for $Q \in E$. The counting function of elliptic pseudoprimes for $Q \in E$ has also been investigated by several authors. The record belongs to Gordon and Pomerance [4], who showed that this function is at most $\exp(\log x - \frac{1}{3}\log L(x))$ for x sufficiently large depending on Q and E. We are not aware of research done on the set of indices n for which F_n can be an elliptic pseudoprime for $Q \in E$.

There are composite integers n which are pseudoprimes for all bases b. They are called Carmichael numbers and there exist infinitely many of them as shown by Alford, Granville and Pomerance in 1994 in [1]. They are also characterized by the property that n is composite, squarefree and $p-1 \mid n-1$ for all prime factors p of n. This characterization is referred to as the *Korselt criterion.*

Analogously, given a fixed curve E having CM by $\mathbb{Q}(\sqrt{-d})$, a composite integer n which is an elliptic pseudoprime for all points Q of infinite order on E is called an elliptic Carmichael number for E. Fix $d \in D$. The authors of [2] defined the following elliptic Korselt criterion which ensures that n is an elliptic Carmichael number for any E with CM by $\mathbb{Q}(\sqrt{-d})$ provided that $(N, \Delta_E) = 1$.

Theorem 1.1. *(EPT) Let N be squarefree, coprime to 6, composite, with an odd number of prime factors p all satisfying $(-d|p) = -1$ and $p+1 \mid N+1$. Then N is an elliptic Carmichael number for any E with CM by $\mathbb{Q}(\sqrt{-d})$ provided that $(N, \Delta_E) = 1$.*

We call positive integers N satisfying the first condition of Theorem 1.1 *elliptic Korselt for* $\mathbb{Q}(\sqrt{-d})$. In [2], it is shown that there are infinitely many elliptic Korselt numbers for $\mathbb{Q}(\sqrt{-d})$ for all $d \in D$ under some believed conjectures from the distribution of prime numbers. It was recently shown by Wright [10] that the number of elliptic Carmichael numbers up to x is

$$\geq \exp\left(\frac{K \log x}{(\log\log\log x)^2}\right) \quad \text{with some positive constant} \quad K$$

for all $x > 100$.

Here, we fix $d \in D := \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$ and look at the set of numbers

$$\mathcal{N}^{(d)} = \{n : F_n \text{ is elliptic Korselt for } \mathbb{Q}(\sqrt{-d})\}.$$

It is easy to prove that $\mathcal{N}^{(1)} = \emptyset$. Namely, since $F_{2n+1} = F_n^2 + F_{n+1}^2$, it follows that if $r \geq 5$ is an odd prime, then all prime factors of F_r are congruent to 1 modulo 4. In particular, $(-1|p) = 1$ for all prime factors p of F_r. Since $F_r \mid F_n$ for all $r \mid n$, then the primes $p|F_r$ (recall that they all satisfy $(-1|p) = 1$) would divide F_n but that is impossible since F_n is Korselt and its prime factors must satisfy $(-1|p) = -1$. This shows that if $n \in \mathcal{N}^{(1)}$, then n cannot have prime factors $r \geq 5$, therefore $n = 2^a \cdot 3^b$, which is impossible since F_n must be coprime to 6. It is likely that $\mathcal{N}^{(d)}$ is finite for all $d \in D\backslash\{1\}$ (or even empty) but we do not know how to prove such a strong result. Instead, we settle for a more modest goal and prove that $\mathcal{N}^{(d)}$ is of asymptotic density 0. For a subset $\mathcal{A}$ of the positive integers and a positive real number x put $\mathcal{A}(x) = \mathcal{A} \cap [1, x]$.

2. The result

We prove the following result.

Theorem 2.1. *For $d \in D\backslash\{1\}$, we have*

$$\mathcal{N}^{(d)}(x) \ll \frac{x(\log\log x)^{1/2}}{(\log x)^{1/2}}.$$

Proof. Let $\mathcal{Q}$ be the set of primes $q \equiv 2, 3 \pmod 5$. Let x be a large positive real number and y be some parameter depending on x to be made more precise later. Consider $n \in \mathcal{N}(x)$, where we omit the dependence on d for simplicity. Put $N = F_n$. Our proof uses the fact that N is coprime to 6 but it does not use the fact that $(-d|p) = -1$ for all prime factors p of N. We distinguish several cases.

Case 1. $n \in \mathcal{N}_1(x) = \{n \le x : q \nmid n \text{ for any } q \in \mathcal{Q} \cap (y, x)\}$.

By Brun's sieve (see, for example, Theorem 2.3 on Page 70 in [5]), we have

$$\#\mathcal{N}_1(x) \ll x \prod_{\substack{p \in \mathcal{Q} \\ y \le p \le x}} \left(1 - \frac{1}{p}\right) \ll x \left(\frac{\log y}{\log x}\right)^{1/2}. \tag{2.1}$$

From now on, we work with $n \in \mathcal{N}(x) \backslash \mathcal{N}_1(x)$, so there exists $q \in \mathcal{Q}$ with $q \ge y$ such that $q \mid n$. Since such $q \equiv 2, 3 \pmod 5$, it follows that $F_q \equiv -1 \pmod q$. Furthermore, let p be any prime factor of F_q. Then $p \equiv \pm 1 \pmod q$. Since $F_q \equiv -1 \pmod q$, at least one of the prime factors p of F_q has the property that $p \equiv -1 \pmod q$. Thus, $q \mid p + 1$. Since $p + 1 \mid F_n + 1$, we get that $q \mid F_n + 1$. Note that $4 \nmid n$ because otherwise F_n is a multiple of $F_4 = 3$, which is not possible. We now use the fact that

$$F_n + 1 = F_{(n+\delta)/2} L_{(n-\delta)/2},$$

for some $\delta \in \{\pm 1, \pm 2\}$ such that $n \equiv \delta \pmod 4$. Thus,

$$q \mid F_{(n+\delta)/2} L_{(n-\delta)/2} \mid F_{n-\delta} F_{n+\delta}.$$

Hence, either $q \mid F_{n-\delta}$ or $q \mid F_{n+\delta}$. This shows that if we put $z(q)$ for the index of appearance of q in the Fibonacci sequence, then $n \equiv \pm\delta \pmod{z(q)}$.

Put $\mathcal{R} = \{q : z(q) \le q^{1/3}\}$. By a classical argument due to Hooley [6], we have

$$\#\mathcal{R}(t) \ll t^{2/3}. \tag{2.2}$$

Case 2. $\mathcal{N}_2(x) = \{n \in \mathcal{N}_1(x) \backslash \mathcal{N}(x) : q \in \mathcal{R}\}$.

If $n \in \mathcal{N}_2(x)$, then $q \mid n$ for some $q > y$ in $\mathcal{R}$. For a fixed q, the number of such $n \le x$ is $\lfloor x/q \rfloor \le x/q$. Hence,

$$\#\mathcal{N}_2(x) \le \sum_{\substack{y \le q \le x \\ q \in \mathcal{R}}} \frac{x}{q} \le x \sum_{\substack{q \ge y \\ q \in \mathcal{R}}} \frac{1}{q} \ll \frac{x}{y^{1/3}}, \tag{2.3}$$

where the last estimate follows from estimate (2.2) by the Abel summation formula.

Case 3. $\mathcal{N}_3(x) = \mathcal{N}(x) \backslash \left(\mathcal{N}_1(x) \cup \mathcal{N}_2(x)\right)$.

If $n \in \mathcal{N}_3(x)$, then we saw that there exists $q \ge y$ in $\mathcal{Q} \backslash \mathcal{R}$ dividing n such that $n \equiv \delta \pmod{z(q)}$ for some $\delta \in \{\pm 1, \pm 2\}$. Since $q \equiv 2, 3 \pmod 5$, $z(q)$ divides $q + 1$, therefore q and $z(q)$ are coprime. Fixing q and writing $n = qm$, the congruences $mq \equiv \delta \pmod{z(q)}$ put $m \le x/q$ into one of four possible arithmetic progressions modulo $z(q)$. The number of such integers for a fixed q is therefore at most $4\lfloor x/qz(q) \rfloor + 4 \le 4x/qz(q) + 4$. Summing up the above bound over all $q \le x$ in $\mathcal{Q} \backslash \mathcal{R}$, we get that

$$\#\mathcal{N}_3(x) \le 4 \sum_{\substack{y \le q \le x \\ q \notin \mathcal{R}}} \frac{x}{qz(q)} + 4\pi(x) \le 4x \sum_{q \ge y} \frac{1}{q^{4/3}} + 4\pi(x) \ll \frac{x}{y^{1/3}} + \frac{x}{\log x}. \tag{2.4}$$

Comparing estimates (2.1), (2.3), (2.4), it follows that we should choose y such that

$$y^{1/3} = (\log x / \log y)^{1/2}, \qquad \text{giving} \qquad y = (2/3 + o(1)) \frac{(\log x)^{3/2}}{(\log\log x)^{3/2}}$$

as $x \to \infty$. With this choice for y, we get the desired result from (2.1), (2.3) and (2.4), because

$$\#\mathcal{N}(x) \le \#\mathcal{N}_1(x) + \#\mathcal{N}_2(x) + \#\mathcal{N}_3(x).$$

□

3. Comments and Remarks

If $d \neq 1$, we used neither the condition that $(-d|p) = -1$ for all prime factors p of F_n, nor the condition that F_n is squarefree and has an odd number of prime factors. It is likely that if one can find a way to make use of these conditions, then one can give sharper (smaller) upper bound on $\#\mathcal{N}^{(d)}(x)$ than that of Theorem 2.1. Finally, there are other definitions of elliptic Carmichael numbers N which apply to elliptic curves without CM (see for example [7]). It was shown in [7] that the set of N which are Carmichael for E in that sense is of asymptotic density zero. It would be interesting to show that the set of n such that F_n is elliptic Carmichael in that sense is also a set of asymptotic density zero. The methods of this paper do not seem to shed much light on this modified problem.

4. Acknowledgements

We thank the referee for pointing out a logical mistake in a previous version of this paper. This paper was written during a visit of P. S. to the School of Mathematics of the University of the Witwatersrand. This author thanks this institution for hospitality.

References

[1] W. R. Alford, A. Granville and C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. (2) **139** (1994), 703–722.
[2] A. Ekstrom, C. Pomerance and D. S. Thakur, *Infinitude of elliptic Carmichael numbers*, J. Aust. Math. Soc. **92** (2012), 45–60.
[3] D. M. Gordon, *Pseudoprimes on elliptic curves*, in J. M. DeKoninck and C. Levesque, eds. Number Theory, Proc. Internat. Number Theory Conf., Laval 1987, 291–305, de Gruyter, New York, 1989.
[4] D. M. Gordon and C. Pomerance, *The distribution of Lucas and elliptic pseudoprimes*, Math. Comp. **57** (1991), 825–838.
[5] H. Halberstam and H.-E. Richert, *Sieve methods*, Academic Press, London, UK, 1974.
[6] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **226** (1967), 209–220.
[7] F. Luca and I. E. Shparlinski, *Pseudoprime values of the Fibonacci sequence, polynomials and the Euler function*, Indag. Math. (N.S.) **17** (2006), 611–625.
[8] F. Luca and I. E. Shparlinski, *On the counting function of elliptic Carmichael numbers*, Canad. Math. Bull. **57** (2014), 105–112.
[9] C. Pomerance, *On the distribution of pseudoprimes*, Math. Comp. **37** (1981), 587–593.
[10] T. Wright, *There are infinitely many elliptic Carmichael numbers*, preprint, 2014; available at http://webs.wofford.edu/wrighttj/job/carmichael_elliptic_2.pdf.

MSC2010: Primary 11G20,11Y16 ; Secondary 11T23

School of Mathematics, University of the Witwatersrand, P. O. Box Wits 2050, South Africa
E-mail address: florian.luca@wits.ac.za

Naval Postgraduate School, Applied Mathematics Department, Monterey, CA 93943, USA
E-mail address: pstanica@nps.edu