2014-12-27

On Fibonacci numbers which are elliptic Carmichael

Luca, Florian; St nic , Pantelimon

On Fibonacci numbers which are elliptic Carmichael

Florian Luca
School of Mathematics
University of the Witwatersrand
P. O. Box Wits 2050, South Africa

Mathematical Institute
UNAM Juriquilla
Santiago de Querétaro
76230 Querétaro de Arteaga, Mexico
florian.luca@wits.ac.za

Pantelimon Stănică
Naval Postgraduate School
Applied Mathematics Department
Monterey, CA 93943, USA
pstanica@nps.edu

December 27, 2014

Abstract

Here, we show that if E is a CM elliptic curve with CM field different from $\mathbb{Q}(\sqrt{-1})$, then the set of n for which the nth Fibonacci number F_n is elliptic Carmichael for E 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 [11] shows that the inequality

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

holds for all sufficiently large x. It is conjectured that $\pi_b(x) = x/L(x)^{1+o(1)}$ holds as $x \to \infty$. For the Fibonacci sequence $\{F_n\}_{n\geq 1}$ is was shown in [9] 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.

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 (see [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.

Since elliptic curves have become very important in factoring and primality testing, several authors have defined elliptic pseudoprimes and elliptic Carmichael numbers and proved results about them. To define an elliptic Carmichael number, let E be an elliptic curve over $\mathbb{Q}$ given by the minimal *global Weierstraß equation*:

$$E \ : \ y^2 + A_1xy + A_3y = x^3 + A_2x^2 + A_4x + A_6, \tag{1}$$

and let Δ_E be its discriminant. For each prime p we put

$$a_p = p + 1 - \#E(\mathbb{F}_p),$$

where $E(\mathbb{F}_p)$ is the reduction of E modulo p. If $p \mid \Delta_E$, then $E(\mathbb{F}_p)$ has a singularity and we put

$$a_p = \begin{cases} 0 & \text{for the case of a cusp,} \\ 1 & \text{for the case of a split node,} \\ -1 & \text{for the case of a non–split node.} \end{cases}$$

If $p \nmid \Delta_E$, we have $|a_p| < 2\sqrt{p}$. The L-function associated to E is given by

$$L(s,E) = \prod_{p|\Delta_E} \frac{1}{1-a_p p^{-s}} \prod_{p\nmid\Delta_E} \frac{1}{1-a_p p^{-s}+p^{1-2s}}.$$

The infinite product above is convergent for $\mathrm{Re}(s) > 3/2$ and therefore we can expand it into a series $L(s,E) = \sum_{n\geq 1} a_n n^{-s}$. Following [10] (see also [12]), we say that n is an *E-Carmichael number* if

(*i*) n is not a prime power;

(*ii*) $\gcd(n, \Delta_E) = 1$;

(*iii*) for every $p \mid n$ and every point $P \in E(\mathbb{F}_p)$, we have

$$(n - a_n + 1)P = O_p,$$

where in the above both the equation and the group law are considered in $\mathbb{F}_p$.

2 Preliminary observations on E-Carmichael numbers in the CM case

In [10], it was shown that if E has no CM (complex multiplication), then the set of E-Carmichael numbers is of asymptotic density zero. Before stating our main result, we make some comments about condition (*iii*) above. It is known that, as a group,

$$E(\mathbb{F}_p) = \mathbb{Z}/e_p\mathbb{Z} \times \mathbb{Z}/d_p\mathbb{Z},$$

for some integers e_p and d_p with $d_p \mid e_p$. In particular, e_p is the exponent of $E(\mathbb{F}_p)$, namely the smallest positive integer k such that

$$kP = O_p$$

holds for all points $P \in E(\mathbb{F}_p)$. So, with these notations, (*iii*) above becomes equivalent to

$$e_p \mid n - a_n + 1 \qquad \text{for all} \qquad p \mid n. \tag{2}$$

It is plain that if we write

$$\#E(\mathbb{F}_p) = u_{p,E} v_{p,E}^2,$$

where $u_{p,E}$ is squarefree, then $u_{p,E} v_{p,E} \mid e_p$. Thus, (2) implies

$$u_{p,E} v_{p,E} \mid n - a_n + 1 \qquad \text{for all} \qquad p \mid n. \tag{3}$$

Condition (3) is weaker than condition (2) but has the advantage that it depends only on the arithmetic of $p - a_p + 1 = \#E(\mathbb{F}_p)$ and not on the group structure of $E(\mathbb{F}_p)$. When E has complex multiplication by $\mathbb{Q}(\sqrt{-d})$ ($d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$), condition (iii) becomes easier in some cases. Let p be a prime factor of n and suppose additionally that we have $(-d|p) = -1$, where $(a|p)$ denotes the Legendre symbol of a with respect to p. Then $a_p = 0$, so, in particular, $\#E(\mathbb{F}_p) = p + 1$. Furthermore, if there exists such a prime p with the property that $p \| n$ (that is, $p \mid n$ and $p^2 \nmid n$), then, writing $n = pm$ with some integer m coprime to p and using the multiplicative property of a_n, we get that

$$a_n = a_p a_m = 0.$$

In particular, in this case $n - a_n + 1 = n + 1$, a number which is independent of E.

3 The main result

In this paper, we assume that E has CM by $\mathbb{Q}(\sqrt{-d})$, where

$$d \in D := \{2, 3, 7, 11, 19, 43, 67, 163\},$$

and look at the set of numbers

$$\mathcal{N}_d = \{n : F_n \text{ is } E\text{-Carmichael}\}.$$

For a subset $\mathcal{A}$ of the positive integers and a positive real number x put $\mathcal{A}(x) = \mathcal{A} \cap [1, x]$.

Theorem 1. *For $d \in D$, we have*

$$\#\mathcal{N}_d(x) \leq \frac{x}{(\log x)^{1/2 + o(1)}} \qquad (x \to \infty).$$

In [5], the authors gave a sufficient condition for a positive integer n to be an elliptic Carmichael number for all E with CM by $\mathbb{Q}(\sqrt{-d})$ resembling the Korselt criterion for Carmichael numbers. In [8], we showed that the counting function of the set of n such that F_n fulfills that criterion is $O(x(\log\log x)^{1/2}/(\log x)^{1/2})$. The upper bound of the present Theorem 1 is only slightly weaker because of the appearance of $o(1)$ in the exponent of $\log x$, but here we are counting the presumably larger set of n such that F_n is elliptic Carmichael for E. In the concluding section of the paper, we make some comments as to why our argument does not work for $d = 1$.

4 The proof of Theorem 1

Let $\rho(d)$ be the period modulo d of $\{F_n\}_{n\geq 1}$. We have

$$\rho(2) = 3, \quad \rho(3) = 8, \quad \rho(7) = 16, \quad \rho(11) = 10, \quad \rho(19) = 18,$$
$$\rho(43) = 88, \quad \rho(67) = 136, \quad \rho(163) = 328.$$

We let $\ell(d) = \rho(d)$ for all $d \in D\backslash\{2\}$, and $\ell(2) = \rho(8) = 12$ for a reason that will be apparent later. For each $d \in D$, we let

$$A(d) = \left\{1 \leq r \leq \ell(d) : \gcd(r, \ell(d)) = 1, \ \left(\frac{-d}{F_r}\right) = -1\right\},$$

and let $a(d) = \#A(d)$. Note that since $\ell(d)$ is always even, $A(d)$ consists only of odd residue classes of integers. If $d = 2$, then $\ell(d) = 12$, so $\gcd(3, r) = 1$ for $r \in A(2)$. For $d \in D\backslash\{2\}$, since $F_r \equiv F_{r+\ell(d)} \pmod{d}$, we may always assume in the calculation of the elements of $A(d)$ that r is not a multiple of 3, so, in particular, F_r is odd therefore the Jacobi symbol appearing in the definition of $A(d)$ is well defined. For example, $7 \in A(d)$ for $d \in \{2, 7, 11, 19\}$ since $F_7 = 13$, and

$$\left(\frac{-2}{13}\right) = \left(\frac{-7}{13}\right) = \left(\frac{-11}{13}\right) = \left(\frac{-19}{13}\right) = -1,$$

whereas $13 \in A(d)$ for $d \in \{3, 43, 67, 163\} \subset D$ because $F_{13} = 233$, and

$$\left(\frac{-3}{233}\right) = \left(\frac{-43}{233}\right) = \left(\frac{-67}{233}\right) = \left(\frac{-163}{233}\right) = -1.$$

Computing we have

$$a(2) = 2, \quad a(3) = 2, \quad a(7) = 4, \quad a(11) = 2, \quad a(19) = 4,$$
$$a(43) = 20, \quad a(67) = 32, \quad a(163) = 80.$$

Let x be a large positive real number and $y \leq x$ 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. In fact, in what follows, $\mathcal{N}_i(x)$ will be subsets of $\mathcal{N}(x)$ for $i = 1, 2, \ldots$ labeled increasingly as they appear. Let $\mathcal{Q}_d$ be the set of primes $q \equiv r \pmod{\ell(d)}$ for $r \in A(d)$ and $d \in D$.

We distinguish several cases.

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

By the sieve and the prime number theorem in arithmetic progressions, we have

$$\#\mathcal{N}_1(x) \ll x \prod_{\substack{p \in \mathcal{Q}_d \\ y < p < x}} \left(1 - \frac{1}{p}\right) \ll x \left(\frac{\log y}{\log x}\right)^{a(d)/\phi(\ell(d))} \ll x \left(\frac{\log y}{\log x}\right)^{1/2}, \quad (4)$$

where we used the fact that $a(d)/\phi(\ell(d)) = 1/2$ for all $d \in D \backslash \{19\}$, whereas $a(19)/\phi(\ell(19)) = 2/3 > 1/2$.

Case 2. $n \in \mathcal{N}_2(x) = \{n \leq x : q^2 \mid n \text{ for some } q \in (y, x)\}$.

To estimate $\#\mathcal{N}_2(x)$, we fix $q \in (y, x)$ and note that the number of $n \leq x$ such that $q^2 \mid n$ is $\lfloor x/q^2 \rfloor \leq x/q^2$. Summing this up for $q > y$, we get

$$\#\mathcal{N}_2(x) \leq \sum_{y < q < x} \frac{x}{q^2} \leq x \sum_{m \geq y} \frac{1}{m^2} \ll \frac{x}{y}. \quad (5)$$

From now on, we assume that $n \in \mathcal{N}(x) \backslash (\mathcal{N}_1(x) \cup \mathcal{N}_2(x))$. Then there exists $q \in \mathcal{Q}_d \cap (y, x)$ with $q \| n$. Let q be the minimal such prime. Since $q \equiv r \pmod{\ell(d)}$ for some $r \in A(d)$, we get that $F_q \equiv F_r \pmod{d}$. In particular,

$$\left(\frac{-d}{F_q}\right) = \left(\frac{-d}{F_r}\right) = -1.$$

Indeed, this is not quite immediate but it can be shown in the following way (where one sees the reason we chose the definition of $\ell(d)$ the way we did). If d is odd, then since F_q and F_r are congruent to 1 modulo 4, we have

$$\left(\frac{-d}{F_q}\right) = \left(\frac{-1}{F_q}\right)\left(\frac{d}{F_q}\right) = \left(\frac{d}{F_q}\right) = \left(\frac{F_q}{d}\right), \tag{6}$$

where for the last equality we used quadratic reciprocity. The same argument works with q replaced by r to give

$$\left(\frac{-d}{F_r}\right) = \left(\frac{F_r}{d}\right), \tag{7}$$

and now the numbers shown at (6) and (7) are equal because $F_q \equiv F_r \pmod{d}$. Finally, when $d = 2$, the value of $(-d|m)$ for odd m only depends on the class of m modulo 8, and $F_q \equiv F_r \pmod{8}$.

Having concluded that $(-d|F_q) = -1$, we conclude that F_q must have a prime factor p such that $(-d|p) = -1$ and the exponent of p in the factorization of F_q is odd. Let p be the smallest such prime factor of F_q. Let $\nu_p(m)$ be the exponent of p in the factorization of the positive integer m. Let $\nu_p(F_q) = t$ with t odd.

Case 3. $n \in \mathcal{N}_3(x) = \{n \le x : \nu_p(F_n) > \nu_p(F_q)\}$.

In this case, $p \mid F_q$ and $p \mid F_n/F_q$. Writing $n = mq$, it is known that this last condition implies that $p \mid m$. Since also $p \mid F_q$, it follows that $p \equiv \pm 1 \pmod{q}$. Thus, n has two prime factors, $q \in (y, x)$ and $p \equiv \pm 1 \pmod{q}$. Fixing p and q, the number of such $n \le x$ is $\lfloor x/pq \rfloor \le x/pq$. Summing up first over p while keeping q fixed, then over q, we get that

$$\begin{aligned} \#\mathcal{N}_3(x) &\le \sum_{\substack{y<q<x \\ p\le x \\ p\equiv\pm 1 \pmod{q}}} \frac{x}{pq} \ll x \sum_{y<q<x} \frac{1}{q} \sum_{\substack{p\le x \\ p\equiv\pm 1 \pmod{q}}} \frac{1}{p} \\ &\ll x \sum_{y<q} \frac{\log\log x}{q\phi(q)} \ll x \log\log x \sum_{m\ge y} \frac{1}{m(m-1)} \\ &\ll \frac{x \log\log x}{y}. \end{aligned} \tag{8}$$

From now on, we assume that $n \in \mathcal{N}(x)\backslash(\mathcal{N}_1(x) \cup \mathcal{N}_2(x) \cup \mathcal{N}_3(x))$. In this case, $F_n = p^t m$, with some odd t. Since a_n is multiplicative, $a_p = 0$ and

t is odd, we get that $a_{F_n} = a_{p^t} a_m = 0$. Here, we used the fact that $a_{p^t} = 0$, which follows because upon writing $a_p = \alpha + \beta$ for some complex numbers $\alpha,\ \beta$ with $\alpha\beta = p$ (here, $\{\alpha, \beta\} = \{-\sqrt{p}, \sqrt{p}\}$ because their sum is zero), then

$$a_{p^t} = \frac{\alpha^{t+1} - \beta^{t+1}}{\alpha - \beta} = 0,$$

where the last equality holds because $t+1$ is even and $\alpha = -\beta$. Thus, $F_n - a_{F_n} + 1 = F_n + 1$. We observe that

$$F_n + 1 = F_{(n+\delta)/2} L_{(n-\delta)/2} \quad \text{where} \quad \delta \in \{\pm 1, \pm 2\} \quad \text{with} \quad n \equiv \delta \pmod 2.$$

Here, $\{L_m\}_{m \geq 0}$ is the Lucas companion of the Fibonacci sequence given by $L_0 = 2,\ L_1 = 1$ and $L_{m+2} = L_{m+1} + L_m$ for all $m \geq 0$. More precisely,

$$\begin{aligned} F_{4k} + 1 &= F_{2k-1} L_{2k+1}, & F_{4k+1} + 1 &= F_{2k+1} L_{2k}, \\ F_{4k+2} + 1 &= F_{2k+2} L_{2k}, & F_{4k+3} + 1 &= F_{2k+1} L_{2k+2} \end{aligned}$$

(see, for example, [2]). Now clearly,

$$F_{(n+\delta)/2} L_{(n-\delta)/2} \mid F_{n+|\delta|} F_{n-|\delta|} \mid F_{3(n^2-\delta^2)}.$$

Indeed, the first divisibility follows from the fact that $F_{2m} = F_m L_m$ for all positive integers m. For the second one, note that

$$\gcd(F_{n+|\delta|}, F_{n-|\delta|}) = F_{\gcd(n+|\delta|, n-|\delta|} \mid F_{2|\delta|}.$$

If $|\delta| = 1$, then $F_{2|\delta|} = F_2 = 1$, so F_{n+1} and F_{n-1} are coprime and each divides F_{n^2-1}, therefore so does their product. If $|\delta| = 2$, then $F_{2|\delta|} = F_4 = 3$, so either F_{n+2} and F_{n-2} are coprime, in which case their product divides F_{n^2-4} and also $F_{3(n^2-4)}$, or they are each multiples of 3. This happens if $n \equiv 2 \pmod 4$. In that case, at most one of $n+2$ and $n-2$ is a multiple of 3, therefore either $3 \| F_{n+2}$, or $3 \| F_{n-2}$. It now follows easily that

$$\nu_3(F_{3(n^2-4)}) > \max\{\nu_3(F_{n+2}), \nu_3(F_{n-2}\},$$

so it follows that $F_{n+2} F_{n-2} \mid F_{3(n^2-4)}$.

We now write $P(m)$ for the largest prime factor of m, we put

$$z := \exp\left(\frac{\log x \log\log\log x}{\log\log x}\right),$$

and continue with our cases.

Case 4. $n \in \mathcal{N}_4(x) = \{n \le x : P(n) \le z\}$.

In classical notations, $\#\mathcal{N}_4(x) = \Psi(x,z)$. By known estimates from the theory of smooth numbers (see [4]), we have that

$$\#\mathcal{N}_4(x) \le \frac{x}{\exp((1+o(1))u\log u)}, \qquad \text{where} \qquad u = \frac{\log x}{\log z} \qquad (x \to \infty).$$

For us, $u = \log\log x/\log\log\log x$, so $u\log u = (1+o(1))\log\log x$ as $x \to \infty$. Thus, clearly,

$$\#\mathcal{N}_4(x) \ll \frac{x}{(\log x)^{1/2}}. \tag{9}$$

From now on, we assume that

$$n \in \mathcal{N}(x) \setminus \left(\mathcal{N}_1(x) \cup \mathcal{N}_2(x) \cup \mathcal{N}_3(x) \cup \mathcal{N}_4(x)\right).$$

We write $n = Pm$, where $P = P(n) > z$. Put $w = \exp((\log x)^{1/2})$ and let us treat the case:

Case 5. $n \in \mathcal{N}_5(x) = \{n \le x : m \le w\}$.

We fix m. Then $P \le x/m$, so there are $\pi(x/m)$ choices for P. Since

$$\pi(x/m) \ll \frac{x}{m\log(x/m)} \le \frac{x}{m\log z} = \frac{x\log\log x}{m\log x},$$

we get that

$$\begin{aligned} \#\mathcal{N}_5(x) &\ll \sum_{m\le w} \frac{x\log\log x}{m\log x} = \frac{x\log\log x}{\log x}\sum_{m\le w}\frac{1}{m} \\ &\ll \frac{x\log\log x\log w}{\log x} = \frac{x\log\log x}{(\log x)^{1/2}}. \end{aligned} \tag{10}$$

From now on,

$$n \in \mathcal{N}_6(x) = \mathcal{N}(x) \setminus \left(\bigcup_{i=1}^{5}\mathcal{N}_i(x)\right).$$

Let $n = Pm$, $P = P(n) \geq y$, $m > w$. We fix m. Then $P \leq x/m$. Let p be the largest prime factor of F_m. Then $p \geq m - 1$ by Carmichael's Primitive Divisor Theorem [3] (in fact, p/m tends to infinity with m in an effective way by a recent result of Stewart [13], but we shall not need this). Write $p - a_p + 1 = u_{p,E} v_{p,E}^2$. Then, since $|a_p| < 2\sqrt{p}$, we get that

$$u_{p,E} v_{p,E} \geq \sqrt{p - a_p + 1} \gg p^{1/2} \gg m^{1/2}.$$

Condition (3) now gives

$$u_{p,E} v_{p,E} \mid F_n + 1 \mid F_{3(n^2 - \delta^2)},$$

which implies

$$z(u_{p,E} v_{p,E}) \mid 3(n^2 - \delta^2).$$

Here and in what follows, for a positive integer m we write $z(m)$ for the order of appearance of m in the Fibonacci sequence, namely the smallest positive integer k such that $z(m) \mid F_k$. This always exists and has the property that if $m \mid F_\ell$, then $z(m) \mid \ell$. Let $z(u_{p,E} v_{p,E}) = f_E(m)$, a number that depends only on E and m. Since $u_{p,E} v_{p,E} \gg m^{1/2}$, we have $f(m) \gg \log m$. Also,

$$f(m) \mid 3(n^2 - \delta^2).$$

This shows that

$$P^2 m^2 \equiv \delta^2 \pmod{f(m)/\gcd(3, f(m))}.$$

Put $g(m) = f(m)/\gcd(3, f(m))$. If $|\delta| = 1$, then m is odd and invertible modulo $g(m)$, and we get that P^2 is fixed modulo $g(m)$. If $|\delta| = 2$, then m is even, and P^2 is fixed modulo $h(m) = f(m)/\gcd(12, f(m))$. So, in both cases, P^2 is fixed modulo $h(m)$. This puts P in at most $O(\tau(h(m)))$ arithmetic progressions modulo $h(m)$, therefore $O(\tau(f(m)))$ arithmetic progressions modulo $f(m)$. Here, τ is the number of divisors function. To count such P's we distinguish three cases:

(*i*) If $f(m) < z^{1/2}$, we then have that for each fixed progression say a modulo $f(m)$, the number of such primes $P \leq x/m$ is at most

$$\begin{aligned} \pi(x/m; f(m), a) &\ll \frac{x}{m\phi(f(m)) \log(x/mf(m))} \ll \frac{x \log\log x}{mf(m) \log(z^{1/2})} \\ &\ll \frac{x(\log\log x)^2}{mf(m) \log x}. \end{aligned}$$

Here, we used the Brun-Titchmarsh theorem to bound the number of the primes in an arithmetic progression up to x/m, the minimal order $\phi(k) \gg k/\log\log k$ of the Euler function with $k = f(m) < z^{1/2}$ and the fact that

$$\frac{x}{mf(m)} \geq \frac{P}{z^{1/2}} \geq z^{1/2}.$$

Thus, the number of such primes over all progressions modulo $f(m)$ is at most

$$\begin{aligned} &\ll \frac{x(\log\log x)^2 \tau(f(m))}{mf(m)\log x} \ll \frac{x(\log\log x)^2}{mf(m)^{1+o(1)}\log x} \\ &\ll \frac{x(\log\log x)^2}{m(\log x)^{3/2+o(1)}} \end{aligned}$$

as $x \to \infty$, where we used the fact that $\tau(k) = k^{o(1)}$ as $k \to \infty$, as well as the fact that $f(m) \gg \log m \geq \log w = (\log x)^{1/2}$. Summing up over m and using the fact that

$$\sum_{m \leq x} \frac{1}{m} = \log x + O(1),$$

we get a bound of

$$\frac{x}{(\log x)^{1/2+o(1)}} \qquad (x \to \infty). \tag{11}$$

(ii) If $z^{1/2} \leq f(m) < x/m$, then the number of such primes in one progression is at most $x/mf(m) + 1 \leq 2x/mf(m) \ll x/mz^{1/2}$. Summing up over all progressions modulo $f(m)$, the number of such possibilities is at most

$$\ll \frac{x\tau(f(m))}{mz^{1/2}}.$$

Since $f(m) \leq 3x^2$, using the maximal order of the divisor function $\exp(O(\log x/\log\log x))$ for $k \leq 3x^2$, we see that

$$\frac{\tau(f(m))}{z^{1/2}} \leq \exp(O(\log x/\log\log x) - (\log z)/2) < \frac{1}{z^{1/3}}$$

for all sufficiently large x. Thus, the number of such possibilities is at most

$$\frac{x}{mz^{1/3}}.$$

Summing up over m, we get

$$\frac{x \log x}{z^{1/3}}. \tag{12}$$

(*iii*) If $x/m \le f(m) < 3x^2$, then each progression contains at most one such prime. So, for each fixed m, there are at most $\tau(f(m))$ such possibilities. Summing up over all $m \le x/z$, we get a number of possibilities at most

$$\frac{x}{z} \exp(O(\log x/\log\log x)) < \frac{x}{z^{1/2}}. \tag{13}$$

Summarizing the above calculations (11), (12) and (13), the number of $n \in \mathcal{N}_6(x)$ is at most

$$\#\mathcal{N}_6(x) \ll \frac{x}{(\log x)^{1/2+o(1)}} + \frac{x \log x}{z^{1/3}} + \frac{x}{z^{1/2}} \ll \frac{x}{(\log x)^{1/2+o(1)}} \qquad (x \to \infty). \tag{14}$$

We now choose $y = (\log x)^{1/2}$, and the conclusion follows from (4), (5), (8), (9), (10), (14) and the fact that

$$\#\mathcal{N}(x) \le \sum_{i=1}^{6} \#\mathcal{N}_i(x).$$

5 Comments and Remarks

We make some comments on the case $d = 1$. From the remarks preceding the statement of our theorem, if n is a E-Carmichael number then we can exploit well the CM assumption provided that we can find primes p such that $p \| n$ or $\nu_p(n)$ odd, such that $(-d|p) = -1$, because then $n - a_n + 1 = n + 1$. In the case $d = 1$, such primes are the primes $p \equiv 3 \pmod 4$. However, if F_n is a Fibonacci number of odd index and coprime to 3 (otherwise F_n is even), then every prime factor of F_n is congruent to 1 modulo 4. This is easy to see by writing $n = 2t + 1$, and using $F_{2t+1} = F_t^2 + F_{t+1}^2$ and the fact that F_t and F_{t+1} are coprime. Thus, for $d = 1$ and for all n odd and coprime to 6 (a positive proportion of them), there are no prime factors p of F_n with $(-d|p) = (-1|p) = -1$, so we cannot exploit this aspect of the CM condition. In particular, we cannot conclude that $a_{F_n} = 0$ for most n,

and then $F_n - a_{F_n} + 1$ does not have the same nice property as $F_n + 1$ has that it factors as a product of some Fibonacci and Lucas numbers which we successfully exploited in our proof of Theorem 1. Obviously, there might be other aspects of the CM condition for $d = 1$ which we have overlooked and which may be invoked to prove that the set of n for which F_n is E-Carmichael is of asymptotic density zero, but we leave such a task to the reader. Finally, we point out that several authors have treated the more coarse notion of an $P \in E$ pseudoprime, which is a composite integer n such that $(n - a_n + 1)P = O_p$ for all $p \mid n$ and a fixed $P \in E(\mathbb{Q})$ of infinite order (see [5], [6], [7]), and proved that they are of asymptotic density zero. It makes sense to ask the same question for the set of n such that F_n is an $P \in E$ pseudoprime, but we have no idea how to attack this question.

6 Acknowledgements

This paper was written during a visit of P. S. to the School of Mathematics of the University of the Witwatersrand in 2014. This author thanks the 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] Y. Bugeaud, F. Luca, M. Mignotte and S. Siksek, "Fibonacci numbers at most one away from a perfect power", *Elem. Math.* **63** (2008), 65–75.

[3] R. D. Carmichael, "On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$". *Ann. of Math. (2)* **15** (1913/14), no. 1-4, 30–70.

[4] E. R. Canfield, P. Erdős and C. Pomerance, "On a problem of Oppenheim concerning "Factorisatio Numerorum"", *J. Number Theory* **17** (1983), 1–28.

[5] A. Ekstrom, C. Pomerance and D. S. Thakur, "Infinitude of elliptic Carmichael numbers", *J. Aust. Math. Soc.* **92** (2012), 45–60.

[6] 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.

[7] D. M. Gordon and C. Pomerance, "The distribution of Lucas and elliptic pseudoprimes", *Math. Comp.* **57** (1991), 825–838.

[8] F. Luca and P. Stănică, "On Fibonacci numbers which are elliptic Korselt numbers", in P. Alexander, C. Ballot, W. Webb, eds. *Proc. of the XVI International conference on Fibonacci numbers and applications*, Rochester, 2014, to appear.

[9] 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.

[10] F. Luca and I. E. Shparlinski, "On the counting function of elliptic Carmichael numbers", *Canad. Math. Bull.* **57** (2014), 105–112.

[11] C. Pomerance, "On the distribution of pseudoprimes", *Math. Comp.* **37** (1981), 587–593.

[12] J. H. Silverman, "Elliptic Carmichael numbers and elliptic Korselt criteria," arxiv:1108.3830.

[13] C. L. Stewart, "On divisors of Lucas and Lehmer numbers", *Acta Math.* **211** (2013), 291–314.