On the local behavior of the order of appearance in the Fibonacci sequence

Florian Luca
Fundación Marcos Moshinsky, UNAM
Circuito Exterior, C.U., Apdo. Postal 70-543
Mexico D.F. 04510, Mexico
fluca@matmor.unam.mx

Carl Pomerance
Mathematics Department, Dartmouth College,
Hanover, NH 03755, USA
carl.pomerance@dartmouth.edu

August 15, 2013

Abstract

Let $z(N)$ be the order of appearance of N in the Fibonacci sequence. This is the smallest positive integer k such that N divides the kth Fibonacci number. We show that each of the 6 total possible orderings among $z(N)$, $z(N+1)$, $z(N+2)$ appears infinitely often. We also show that for each nonzero even integer c and many odd integers c the equation $z(N) = z(N+c)$ has infinitely many solutions N, but the set of solutions has asymptotic density zero. The proofs use a result of Corvaja and Zannier on the height of a rational function at $\mathcal{S}$-unit points as well as sieve methods.

1 Introduction

Let $\{F_k\}_{k\geq 0}$ be the Fibonacci sequence given by $F_0 = 0$, $F_1 = 1$ and $F_{k+2} = F_{k+1} + F_k$ for all $k \geq 0$. For a positive integer n we put $z(n)$ for the index of appearance of n in the Fibonacci sequence which is the minimal positive integer k such that $n \mid F_k$. It is known that this always exists. Furthermore, $n \mid F_k$ if and only if $z(n) \mid k$. Here, we look at the local behavior of the function $z(n)$. We do not expect the function $z(n)$ to exhibit some prescribed monotonicity pattern. Rather we expect it to behave randomly on intervals of fixed length with an arbitrary starting point. Thus, we propose the following conjecture.

Conjecture 1. *For all integers $k \geq 2$ and all permutations $\sigma \in S_k$, there exist infinitely many N such that*

$$z(N + \sigma(1)) < z(N + \sigma(2)) < \cdots < z(N + \sigma(k)). \tag{1}$$

It is clear that the validity of Conjecture 1 for k implies the validity of it for smaller values of k. Our main result is the following:

Theorem 1. *Conjecture 1 holds for $k = 3$.*

Some partial results in the spirit of Theorem 1 appear in [6]. One may also ask about values of N such that $z(N) = z(N+1)$. Or $z(N) = z(N+2)$. For a nonzero integer c put

$$\mathcal{N}_c := \{N : z(N) = z(N + c)\}. \tag{2}$$

Theorem 2. *For each nonzero even integer c and for each odd integer c with $3 \nmid z(c)$, the set $\mathcal{N}_c$ is infinite.*

In particular, each one of the equalities $z(N) = z(N+1)$ and $z(N) = z(N+2)$ holds infinitely often. This answers a question from [5]. (In fact, $z(N) = z(N + c)$ holds infinitely often for each positive c up to 16.)

Even if the set $\mathcal{N}_c$ is infinite, one does not expect it to be too thick. We make this precise in the next result. For a positive real number x and a set $\mathcal{A}$ of positive integers we write $\mathcal{A}(x) = \mathcal{A} \cap [1, x]$.

Theorem 3. *The estimate*

$$\#\mathcal{N}_c(x) = O_c\left(\frac{x}{(\log x)^2}\right) \tag{3}$$

holds for all nonzero c.

We believe that in fact $\#\mathcal{N}_c(x)$ is of order $x/(\log x)^2$, and in the last section of the paper we make some comments about this. Note that Theorem 3 implies that the sum of the reciprocals of the members of $\mathcal{N}_c$ is finite.

Analogues of our theorems hold in the more general setting of binary recurrent sequences (u_n) with $u_0 = 0$, $u_1 = 1$ and with the roots of the associated characteristic polynomial being quadratic units but not roots of unity. In addition, Theorem 3 holds in a still more general setting, for example the estimation of the number of odd integers $n \le x$ for which the multiplicative order of 2 (mod n) is equal to the multiplicative order of 2 (mod $n+2$).

2 Notations, Terminology and Some Preliminary Results

We write $\{L_k\}_{k\ge 0}$ for the Lucas companion of the Fibonacci sequence which is given by $L_0 = 2$, $L_1 = 1$ and $L_{k+2} = L_{k+1} + L_k$ for all $k \ge 0$. Writing $(\alpha, \beta) := ((1+\sqrt{5})/2, (1-\sqrt{5})/2)$ for the two roots of the characteristic equation $x^2 - x - 1 = 0$, the Binet formulas for the Fibonacci and Lucas numbers are

$$F_k = \frac{\alpha^k - \beta^k}{\alpha - \beta} \qquad \text{and} \qquad L_k = \alpha^k + \beta^k \qquad \text{for all} \qquad k \ge 0. \tag{4}$$

Both sequences $\{F_k\}_{k\ge 0}$ and $\{L_k\}_{k\ge 0}$ can be extended to negative indices either allowing k to be negative in the Binet formula (4), or by extending the recurrence relation for the Fibonacci and Lucas numbers to negative indices. Once this is done, we have $F_{-k} = (-1)^{k-1}F_k$ and $L_{-k} = (-1)^k L_k$ for all positive integers k. There are many formulas relating the Fibonacci and Lucas numbers such as $F_{2k} = F_k L_k$ which holds for all integers k and

$$F_u + (-1)^{(u-v)/2} F_v = F_{(u+v)/2} L_{(u-v)/2} \quad \text{when} \quad u \equiv v \pmod 2.$$

We will apply this last relation in the following special cases:

$$F_u + \varepsilon F_v = F_{(u+\varepsilon v)/2} L_{(u-\varepsilon v)/2} \quad \text{if} \quad u \equiv v \equiv 0 \pmod 4,\ \varepsilon \in \{\pm 1\}, \tag{5}$$

and

$$F_{2u} + (-1)^u \varepsilon = F_{u-\varepsilon} L_{u+\varepsilon} \quad \text{for all} \quad u. \tag{6}$$

We shall also use classical divisibility properties of the Fibonacci and Lucas numbers. We summarize them in the following lemma.

Lemma 2. *Let u and v be positive integers and $d := \gcd(u,v)$. Then*

(i) $\gcd(F_u, F_v) = F_d$;

(ii) $\gcd(L_u, L_v) = L_d$ *if both u/d and v/d are odd; else,* $\gcd(L_u, L_v)$ *is* 2 *or* 1 *according to whether $3 \mid d$ or not, respectively;*

(iii) $\gcd(F_u, L_v) = L_d$ *if u/d is even and v/d is odd; else,* $\gcd(F_u, L_v)$ *is* 2 *or* 1 *according to whether $3 \mid d$ or not, respectively.*

We shall also use the Primitive Divisor Theorem of Carmichael [2], which states that if $n \notin \{1,2,6,12\}$, then there is a prime factor p of F_n having $z(p) = n$. Finally we use the fact that for all positive integers a, b we have

$$\text{lcm}[z(a), z(b)] = z(\text{lcm}[a,b]).$$

Throughout the paper, we use the Landau symbols O and o as well as the Vinogradov symbols $\ll$, $\gg$ and $\asymp$ with their regular meaning. The constants implied by them might depend on some parameters to be fixed throughout the proofs like a, or c, or k, etc. We use p, q and P, Q with or without subscripts for prime numbers.

3 On the index of appearance of shifts of Fibonacci numbers

Here, we prove the following result.

Proposition 3. *Let $a \in \mathbb{Z}$ be such that $|a|$ is not a Fibonacci number. Then*

$$\lim_{n\to\infty} \frac{z(F_n+a)}{n^2} = \infty.$$

Proof. Put $m := z(F_n + a)$. Then $F_n + a \mid F_m$. Assume that $n > 0$ satisfies $F_{n-2} > |a|$. Since $|a| \geq 4$, it follows that $n \geq 7$. Then

$$F_n + a > F_n - F_{n-2} = F_{n-1}, \tag{7}$$

so $m > n-1$. If $m = n$, then estimate (7) shows that $F_n + a$ is a divisor of F_n which exceeds $F_{n-1} = (F_{n-1}/F_n)F_n > F_n/2$. But then we must have $F_n + a = F_n$, which is false. So, $m > n$.

Assume that $m \leq Kn^2$ for some fixed K. We need to show that there are only finitely many possibilities for n. Write

$$m = qn + r, \quad \text{where} \quad 1 \leq q := \lfloor m/n \rfloor \leq Kn, \qquad \text{and} \qquad 0 \leq r \leq n-1. \tag{8}$$

We fix the parity of n. That is, we assume that $n \equiv c \pmod 2$, where $c \in \{0, 1\}$. Observe that, by formula (4),

$$\begin{aligned} F_n + a &= \frac{\alpha^n - \beta^n}{\sqrt{5}} + a = \frac{\alpha^{-n}}{\sqrt{5}}\left(\alpha^{2n} + \sqrt{5}a\alpha^n - (-1)^c\right) \\ &= \frac{\alpha^{-n}}{\sqrt{5}}\left(\alpha^n - z_1\right)\left(\alpha^n - z_2\right), \end{aligned} \tag{9}$$

where

$$z_1, z_2 := \frac{-\sqrt{5}a \pm \sqrt{5a^2 + 4(-1)^c}}{2}.$$

Write $5a^2 + 4(-1)^c =: db^2$, where d is squarefree. It is clear that $d > 0$. Since all positive integer solutions (x, y) of the equation $x^2 - 5y^2 = \pm 4$ are of the form $(x, y) = (L_k, F_k)$ for some $k \geq 1$, and $|a|$ is not a Fibonacci number, it follows that $d > 1$. It is clear that d is coprime to 5. Putting $\mathbb{K} := \mathbb{Q}(\sqrt{5}, \sqrt{d})$, we get that $\mathbb{K}$ is real and of degree 4 over $\mathbb{Q}$. The field $\mathbb{K}$ is also normal and its Galois group G is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. It is also clear that z_1 and α are multiplicatively independent. Indeed, to see this observe that $\alpha \in \mathbb{Q}(\sqrt{5})$ and $z_1^2 \in \mathbb{Q}(\sqrt{5d})$. Thus, if for some integers (r, s) not both zero we would have $\alpha^r = z_1^{2s}$, then this number is in $\mathbb{Q}(\sqrt{5}) \cap \mathbb{Q}(\sqrt{5d}) = \mathbb{Q}$. Since

$\alpha^r \in \mathbb{Q}$ implies that $r = 0$, and the relation $\alpha^r = z_1^{2s}$ with $r = 0$ implies that $s = 0$, we get that $r = s = 0$, which is a contradiction.

Let Γ be the multiplicative group generated inside $\mathbb{K}$ by $\{-1, \alpha, z_1\}$. Since $z_1 z_2 = (-1)^{c+1}$, Γ contains z_2. Put $u_1 := \alpha^n z_1^{-1}$. Since z_1 is a unit, observe that u_1 is an algebraic integer and $u_1 - 1$ is associated to $\alpha^n - z_1$. Since $(F_n + a)/((\alpha^n - z_1)/\sqrt{5})$ is an algebraic integer and

$$F_n + a \mid F_m \mid F_{2m} = \beta^{2m} \frac{\alpha^{4m} - 1}{\sqrt{5}},$$

we get that $\alpha^n - z_1 \mid \alpha^{4m} - 1$, leading to $u_1 - 1 \mid \alpha^{4m} - 1$. We thus get the two relations

$$\alpha^n z_1^{-1} \equiv 1 \pmod{u_1 - 1}, \qquad \text{and} \qquad \alpha^{4m} \equiv 1 \pmod{u_1 - 1}. \tag{10}$$

Here and in what follows, we use the standard convention that two algebraic integers γ and δ are congruent modulo a nonzero algebraic integer η if $(\gamma - \delta)/\eta$ is an algebraic integer. Using formula (8) to replace $4m$ by $4nq + 4r$ in the second congruence in (10), and using also the first congruence in (10) to replace α^n by z_1 modulo $u_1 - 1$, we get the congruence

$$\alpha^{4r} z_1^{4q} \equiv 1 \pmod{u_1 - 1}. \tag{11}$$

Put $v_1 := \alpha^{4r} z_1^{4q}$. Here is a proof that u_1 and v_1 are multiplicatively independent. Since α and z_1 are multiplicatively independent, the equation $(\alpha^n z_1^{-1})^a = (\alpha^{4r} z_1^{4q})^b$ with integers a, b forces $an = 4rb$ and $-a = 4qb$, so either $a = b = 0$ or $qr < 0$, the second option being false. To summarize, $u_1 - 1 \mid v_1 - 1$ and u_1 and v_1 are multiplicatively independent elements of Γ.

We now apply Corollary 1 in [3] to our situation. More precisely, inequality (1.3) in [3] says that for all $\delta > 0$, the inequality

$$\sum_{\mu \in \mathcal{M}_{\mathbb{K}}} \log^- \left(\max\{|u_1 - 1|_\mu, |v_1 - 1|_\mu\} \right) > -\delta \max\{h(u_1), h(v_1)\} \tag{12}$$

holds with finitely many exceptions in the pair (u_1, v_1). Here, $\log^-(\bullet) = \min\{0, \log(\bullet)\}$, $\mathcal{M}_{\mathbb{K}}$ is the set of valuations of $\mathbb{K}$, for $\mu \in \mathcal{M}_{\mathbb{K}}$, $|\bullet|_\mu$ means the corresponding normalized absolute value such that the product formula holds, and $h(\bullet)$ is the Weil height (the definition of which is shown in (19) later in this proof). The normalized absolute values $|\bullet|_\mu$ for us are as follows:

(i) If μ is finite, then it corresponds to some prime ideal π in $\mathbb{K}$ of norm (number of elements of the residue field) equal to p^f for some prime p and some $f \in \{1, 2, 4\}$. Then $|\bullet|_\mu = p^{-(f/4)\mathrm{ord}_\pi(\bullet)}$, where $\mathrm{ord}_\pi(\bullet)$ is the exponent at which π appears in the prime ideal factorization of the fractional ideal generated by the nonzero element $\bullet$ inside $\mathbb{K}$.

(ii) If μ is infinite, then it corresponds to some element $\sigma \in G$, and then $|\bullet|_\mu = |\sigma(\bullet)|^{1/4}$.

Since for us finitely many exceptions (u_1, v_1) means finitely many values for n, we assume that n is sufficiently large such that inequality (12) holds.

Let us see what estimate (12) means for us. Since $u_1 - 1 \mid v_1 - 1$ and both $u_1 - 1$ and $v_1 - 1$ are algebraic integers, it follows that

$$\log^- (\max\{|u_1 - 1|_\mu, |v_1 - 1|_\mu\}) = \log |u_1 - 1|_\mu \quad \text{for finite} \quad \mu \in \mathcal{M}_{\mathbb{K}}. \tag{13}$$

For the remaining four infinite valuations μ, let us notice that the term corresponding to μ in the left-hand side of (12) is 0 unless both $|u_1 - 1|_\mu$ and $|v_1 - 1|_\mu$ are in $(0, 1)$. In this case,

$$|u_1 - 1|_\mu = |\sigma(\alpha)^n \sigma(z_1)^{-1} - 1|^{1/4} \qquad \text{and} \qquad |v_1 - 1|_\mu = |\sigma(\alpha)^{4r} \sigma(z_1)^{4q} - 1|^{1/4},$$

where σ is the element of G corresponding to μ. Using the multiplicative independence of α and z_1 and Baker's theory of lower bounds for nonzero linear forms in logarithms of algebraic numbers (see [7], for example), inequality (8) implies that

$$\log^- (\max\{|u_1 - 1|_\mu, |v_1 - 1|_\mu\}) = O(\log K + \log n), \quad \text{for infinite} \quad \mu \in \mathcal{M}_{\mathbb{K}}, \tag{14}$$

where the constant implied by the above O–symbol depends on a. We may assume that $n > K$ (because K is fixed), and then omit the term $\log K$ in the right–hand side of estimates (14).

Inserting estimates (13) and (14) into (12), we get for some fixed κ (depending on a),

$$\sum_{\substack{\mu \in \mathcal{M}_{\mathbb{K}} \\ \mu \text{ finite}}} \log |u_1 - 1|_\mu + \kappa \log n > -\delta \max\{h(u), h(v)\}. \tag{15}$$

By the product formula, the main term in the left–hand side in estimate (15) is

$$-\sum_{\substack{\mu\in\mathcal{M}_{\mathbb{K}}\\ \mu \text{ infinite}}} \log|u_1-1|_\mu = -\frac{1}{4}\log|N_{\mathbb{K}/\mathbb{Q}}(u_1-1)|,$$

where $N_{\mathbb{K}/\mathbb{Q}}(\bullet)$ is the norm map from $\mathbb{K}$ to $\mathbb{Q}$. Hence, estimate (15) implies that

$$\frac{1}{4}\log|N_{\mathbb{K}/\mathbb{Q}}(u_1-1)| - \kappa\log n < \delta\max\{h(u_1),h(v_1)\}. \tag{16}$$

We now repeat the argument with $u_2 := \alpha^n z_2^{-1} - 1$, which is associated to $\alpha^n - z_2$. Putting $v_2 := \alpha^{4r} z_2^{4q}$, the same argument gives that inequality (16) holds with u_1 and v_1 replaced by u_2 and v_2, respectively. Summing them up, and adjusting κ if necessary, we get

$$\frac{1}{4}\log\left|N_{\mathbb{K}/\mathbb{Q}}\left((u_1-1)(u_2-1)\right)\right| - \kappa\log n \\ < 2\delta\max\{h(u_1),h(v_1),h(u_2),h(v_2)\}. \tag{17}$$

By formula (9), we get easily that

$$\left|N_{\mathbb{K}/\mathbb{Q}}\left((u_1-1)(u_2-1)\right)\right| = 25(F_n+a)^4 > 25F_{n-1}^4 > 25\alpha^{4n-12} > \alpha^{4n-6}, \tag{18}$$

where we used the fact that the inequality $F_k > \alpha^{k-2}$ holds for all $k \geq 3$. Finally, recall that if η is an algebraic number of degree d of minimal polynomial

$$F(X) := a_0\prod_{j=1}^{d}(X-\eta^{(j)})$$

over $\mathbb{Z}[X]$, then

$$h(\eta) := \frac{1}{d}\left(\log a_0 + \sum_{j=1}^{d}\log(\max\{1,|\eta^{(j)}|\})\right). \tag{19}$$

Taking $\eta := u_i$ for $i = 1,\ 2$, all its conjugates are of the form $\sigma(\alpha)^n\sigma(z_i)^{-1}$ for some element $\sigma \in G$. Thus,

$$\log(\max\{1,|\eta^{(j)}|\}) = O(n),$$

for all $j = 1, \ldots, 4$, implying that $h(u_i) = O(n)$ for $i = 1,\ 2$. In the case of $h(v_i)$ for $i = 1,\ 2$, the number n must be replaced by $q+r$, which is bounded above by $(K+1)n \le 2Kn$. Hence, we get

$$\max\{h(u_1), h(u_2), h(v_1), h(v_2)\} = O(Kn), \tag{20}$$

where the constant implied by the above O–symbol depends on a. Inserting estimates (18) and (20) into estimate (17), we get

$$n \log \alpha - \kappa \log n = O(K\delta n).$$

We divide the above estimate by n to get

$$\log \alpha = O(K\delta),$$

that is,

$$\log \alpha < c_1 K \delta$$

holds for all n sufficiently large with some positive constant c_1 depending on a. Hence, $K > c_2\delta^{-1}$, where $c_2 := c_1^{-1} \log \alpha$. Thus, the inequality $K > c_2\delta^{-1}$ holds for all large n, and we get the desired conclusion because $\delta > 0$ was arbitrary. ◻

When $|a|$ is a Fibonacci number, one can show that

$$\liminf_{n\to\infty} \frac{z(F_n + a)}{n^2} = O(1), \tag{21}$$

so Proposition 3 can be seen as a characterization of the Fibonacci numbers. The proof of estimate (21) is based on the analogs of relation (5) for pairs of indices (u, v) which are congruent modulo 2. See the next two sections for some arguments in this style.

4 The Proof of Theorem 1

Of the six possible patterns among $z(N),\ z(N+1),\ z(N+2)$, we distinguish *slopes* (the monotonic patterns), *peaks* (the patterns with a maximum in the middle), and *valleys* (the patterns with a minimum in the middle), respectively.

4.1 Slopes

We start with $N := F_n/F_k$, where k and n are positive integers such that $12 \mid k \mid n$. Put $\ell := n/k$. We also assume that $k \mid \ell$. It is clear that $z(N) \mid n$. By the Primitive Divisor Theorem, there exists a prime $p \mid F_n$ with $z(p) = n$. Thus, $p \mid N$, therefore $z(N) = n$.

Next, let $\varepsilon \in \{\pm 1\}$. Then, by (5),

$$N + \varepsilon = \frac{F_n + \varepsilon F_k}{F_k} = \frac{F_{(n+\varepsilon k)/2} L_{(n-\varepsilon k)/2}}{F_k} = \left(\frac{F_{k(\ell+\varepsilon)/2}}{F_{k/2}}\right)\left(\frac{L_{k(\ell-\varepsilon)/2}}{L_{k/2}}\right). \quad (22)$$

Since $\ell - \varepsilon \geq 5$ is coprime to 6 (in particular, it is odd), it follows by Lemma 2 that both factors in the right–hand side above are integers. The first factor divides $F_{k(\ell+\varepsilon)/2}$ so its index of appearance is a divisor of $k(\ell+\varepsilon)/2$. By the Primitive Divisor Theorem once again, its index of appearance is precisely $k(\ell+\varepsilon)/2$. The second factor divides $F_{k(\ell-\varepsilon)}$, and again by the Primitive Divisor Theorem, its index of appearance equals $k(\ell-\varepsilon)$. Hence, $z(N+\varepsilon)$ must be a multiple of

$$\text{lcm}\left[\frac{k(\ell+\varepsilon)}{2}, k(\ell-\varepsilon)\right] = k(\ell^2 - 1) = \frac{n^2 - k^2}{k}.$$

Here we have used that k is coprime to $\ell^2 - 1$. To see that $z(N+\varepsilon)$ is exactly the above number, it suffices to note that the two factors in the right side of (22) are coprime, which follows from $\gcd(F_{k(\ell+\varepsilon)/2}, L_{k(\ell-\varepsilon)/2}) = 2$ by (iii) of Lemma 2 and both $L_{k(\ell-\varepsilon)/2}$ and $L_{k/2}$ are $2 \pmod 4$ (using $L_m \equiv 2 \pmod 4$ when $6 \mid m$). Hence, $z(N+\varepsilon) = (n^2 - k^2)/k$.

Next, note that

$$N + 2\varepsilon = \frac{F_n + 2\varepsilon F_k}{F_k}.$$

Let $m := z(N + 2\varepsilon)$. We then get that

$$F_n + 2\varepsilon F_k \mid F_k F_m \mid F_k F_{km} \mid F_{kF_k m},$$

where for the last divisibility relation we used repeatedly the fact that if p is any prime and $p^j \mid F_r$, then $p^j F_r \mid F_{p^j r}$. Hence,

$$kF_k m \geq z(F_n + 2\varepsilon F_k),$$

leading to

$$z(N+2\varepsilon) \geq \frac{z(F_n+2\varepsilon F_k)}{kF_k}. \tag{23}$$

Since $2F_k$ is not a Fibonacci number for $k \geq 4$ (in fact, $F_{k+1} < 2F_k < F_{k+2}$ for all $k \geq 3$), it follows that for a fixed k, the right–hand side in estimate (23) above is larger than n^2 for all n sufficiently large by Proposition 3. Hence, for large n, our construction gives

$$z(N+2\varepsilon) > n^2 > \frac{n^2-k^2}{k} = z(N+\varepsilon) > n = z(N),$$

which completes this part of the argument.

4.2 Peaks

This construction is quite similar to the previous one, so we shall only sketch it. We again take $12 \mid k \mid \ell$ and $n := k\ell$. Put $N := 2F_n/F_k = F_n/(F_k/2)$. Again by the Primitive Divisor Theorem, $z(N) = n$.

For $\varepsilon \in \{\pm 1\}$,

$$N+\varepsilon = \frac{F_n+\varepsilon F_k/2}{F_k/2}.$$

Since $k \geq 12$, $F_k/2$ is not a Fibonacci number, therefore Proposition 3 implies, as in the concluding part of the argument from Section 4.1, that $z(N+\varepsilon) > n^2$ for all fixed k and large n.

Also, by (5), we have

$$N+2\varepsilon = \frac{F_n+\varepsilon F_k}{F_k/2} = \frac{F_{(n+\varepsilon k)/2}L_{(n-\varepsilon k)/2}}{F_k/2} = \left(\frac{F_{k(\ell+\varepsilon)/2}}{F_{k/2}/2}\right)\left(\frac{L_{k(\ell-\varepsilon)/2}}{L_{k/2}}\right). \tag{24}$$

Both factors on the right hand side above are integers. By the Primitive Divisor Theorem, the index of appearance of the first factor is $k(\ell+\varepsilon)/2$, and the index of appearance of the second factor is $k(\ell-\varepsilon)$. These two factors in (24) are coprime by the same argument as in Section 4.1. This fact and the calculation of $z(N+\varepsilon)$ from Section 4.1 shows that $z(N+2\varepsilon) = (n^2-k^2)/k$. We now get easily that

$$z(N+\varepsilon) > n^2 > \frac{n^2-k^2}{k} = z(N+2\varepsilon) > n = z(N),$$

which finishes this part of the argument.

4.3 Valleys

We again take $12 \mid k \mid \ell$ and $n := k\ell$. Let $\varepsilon \in \{\pm 1\}$, and put

$$N := \frac{F_n + 1}{F_k - \varepsilon} = \left(\frac{F_{(n-2)/2}}{F_{(k+2\varepsilon)/2}}\right)\left(\frac{L_{(n+2)/2}}{L_{(k-2\varepsilon)/2}}\right), \tag{25}$$

where we used (6). Fix k and let ℓ satisfy the following congruence:

$$\ell \equiv -\varepsilon \pmod{k^2/4 - 1}. \tag{26}$$

Since k is a multiple of 4, the congruence (26) is compatible with $\ell \equiv 0 \pmod{k}$, so there are infinitely many solutions by the Chinese Remainder Lemma. For such solutions ℓ and $n = k\ell$, we have that

$$n = k\ell \equiv \mp 2\varepsilon\ell \equiv \pm 2 \pmod{k/2 \pm \varepsilon},$$

so that both $(n-2)/(k+2\varepsilon)$ and $(n+2)/(k-2\varepsilon)$ are odd integers. Thus, the two factors appearing in the right side of (25) are integers by Lemma 2, and so N is an integer. By the Primitive Divisor Theorem, the index of appearance of the first factor in the right–hand side of (25) is $(n-2)/2$ for large n, and the index of appearance of the second factor is $n+2$. Since $(n-2)/2$ and $n+2$ are coprime, we get that $z(N) = (n^2-4)/2$.

Now by (5) and (6)

$$N + \varepsilon = \frac{F_n + \varepsilon F_k}{F_k - \varepsilon} = \frac{F_{(n+\varepsilon k)/2} L_{(n-\varepsilon k)/2}}{F_{(k+2\varepsilon)/2} L_{(k-2\varepsilon)/2}} = \frac{F_{k(\ell+\varepsilon)/2} L_{k(\ell-\varepsilon)/2}}{F_{k/2+\varepsilon} L_{k/2-\varepsilon}}. \tag{27}$$

The index of appearance of $F_{k(\ell+\varepsilon)/2}$ is $k(\ell+\varepsilon)/2$. If n is sufficiently large, then by the Primitive Divisor Theorem, a primitive prime factor of $F_{k(\ell+\varepsilon)/2}$ will not divide $F_{k-2}F_{k+2}$, which is a multiple of the denominator $F_{(k+2\varepsilon)/2}L_{(k-2\varepsilon)/2}$ appearing in the right side in (27), and so it will divide $N+\varepsilon$. The same is true about the primitive prime factors of $L_{k(\ell-\varepsilon)/2}$. Hence, by the arguments from Section 4.1, $z(N+\varepsilon)$ is a multiple of $(n^2-k^2)/k$. By Lemma 2, the gcd of the two factors in the numerator of the right side of (27) is 2, so $z(N+\varepsilon)$ is a divisor of $2(n^2-k^2)/k$.

Finally,

$$N + 2\varepsilon = \frac{F_n + 2\varepsilon F_k - 1}{F_k - \varepsilon}.$$

Put $m := z(N+2\varepsilon)$. Then $F_n + 2\varepsilon F_k - 1 \mid (F_k - \varepsilon)F_m = F_{(k+2\varepsilon)/2} L_{(k-2\varepsilon)/2} F_m$, so that

$$F_n + 2\varepsilon F_k - 1 \mid F_{k-2}F_{k+2}F_m \mid F_{k^2-4}F_{(k^2-4)m} \mid F_{(k^2-4)F_{k^2-4}m}. \tag{28}$$

In the above calculation, we used the fact that

$$\gcd(F_{k+2}, F_{k-2}) = F_{\gcd(k+2,k-2)} = F_2 = 1.$$

For large k, the number $|2\varepsilon F_k + 1| = 2F_k \pm 1$ is not a Fibonacci number. In fact, $F_{k+1} < 2F_k - 1 < 2F_k + 1 < F_{k+2}$ for all $k \geq 5$. Hence, by Proposition 3 and divisibilities (28), we get that

$$m \geq \frac{z(F_n + 2\varepsilon F_k - 1)}{(k^2-4)F_{k^2-4}} > n^2$$

for all sufficiently large n once k is fixed. Thus, we have

$$z(N+2\varepsilon) > n^2 > \frac{n^2-4}{2} = z(N) > 2\frac{(n^2-k^2)}{k} \geq z(N+\varepsilon),$$

which completes the analysis for this last case.

This proves Theorem 1.

5 The Proof of Theorem 2

This is very similar to the proof of Theorem 1. We may assume that c is positive.

Assume that c is even. Here, we let k be a multiple of 12 such that $c/2 \mid F_{k/2}$. For this, it is enough that $24z(c/2) \mid k$. We let $n := k\ell$ with a large $\ell \equiv 0 \pmod{k}$ and put

$$N := \frac{F_n}{F_k/(c/2)} - \frac{c}{2}.$$

Then

$$N = \frac{F_n - F_k}{F_k/(c/2)} = \left(\frac{F_{k(\ell-1)/2}}{F_{k/2}/(c/2)}\right)\left(\frac{L_{k(\ell+1)/2}}{L_{k/2}}\right), \tag{29}$$

where we used (5). By Lemma 2, both factors in the right–hand side of formula (29) above are integers. By the Primitive Divisor Theorem, for large ℓ the index of appearance of the first factor is $k(\ell-1)/2$ and the index of appearance of the second factor is $k(\ell+1)$. Since ℓ is even, so $\ell \pm 1$ are odd, and k is a multiple of 3, it follows by Lemma 2 that the greatest common divisor of $F_{k(\ell-1)/2}$ and $L_{k(\ell+1)/2}$ is 2. Since $6 \mid k/2$, we get that $2 \| L_{k/2}$ and $2 \| L_{k(\ell+1)/2}$, so, in particular, the second factor in the right–hand side of formula (29) is odd. Hence, these two factors are in fact coprime, showing that

$$z(N) = \operatorname{lcm}\left[\frac{k(\ell-1)}{2}, k(\ell+1)\right] = k(\ell^2-1) = \frac{n^2-k^2}{k}. \tag{30}$$

Similarly,

$$N + c = \frac{F_n}{(F_k/(c/2))} + \frac{c}{2} = \frac{F_n + F_k}{F_k/(c/2)} = \left(\frac{F_{k(\ell+1)/2}}{F_{k/2}/(c/2)}\right)\left(\frac{L_{k(\ell-1)/2}}{L_{k/2}}\right). \tag{31}$$

Proceeding as above, we get that the two numbers appearing in the right–hand side of (31) are integers. Also, for large ℓ, by the Primitive Divisor Theorem, their order of appearances are $k(\ell+1)/2$ and $k(\ell-1)$, respectively. Also, the second factor in (31) is odd, so these two factors are in fact coprime by Lemma 2. Thus,

$$z(N+c) = \operatorname{lcm}\left[\frac{k(\ell+1)}{2}, k(\ell-1)\right] = k(\ell^2-1) = \frac{n^2-k^2}{k} = z(N), \tag{32}$$

which is what we wanted.

To complete the proof we assume that c is odd and $3 \nmid z(c)$. We take k a multiple of $4z(c)$ but not of 3, we take ℓ a multiple of k with $\ell \equiv 1 \pmod 3$, and we take $n = k\ell$. Note that F_n is odd. We put

$$N := \frac{F_n}{2(F_k/c)} - \frac{c}{2} = \frac{F_n - F_k}{2F_k/c} = \left(\frac{F_{k(\ell-1)/2}}{2F_{k/2}/c}\right)\left(\frac{L_{k(\ell+1)/2}}{L_{k/2}}\right), \tag{33}$$

Since $\ell \equiv 1 \pmod 3$ and ℓ is even, the two factors on the right side of (33) are integers. By the Primitive Divisor Theorem, for large ℓ the order of appearance of the first factor is $k(\ell-1)/2$ and the order of appearance of the second factor is $k(\ell+1)$. Finally, by Lemma 2 and the fact that the second factor in (33) is odd, we get that these two factors are coprime. The conclusion now is that formula (30) holds. Now clearly,

$$N+c=\frac{F_n}{2F_k/c}+\frac{c}{2}=\frac{F_n+F_k}{2F_{k/c}}=\left(\frac{F_{k(\ell+1)/2}}{F_{k/2}/c}\right)\left(\frac{L_{k(\ell-1)/2}}{2L_{k/2}}\right). \tag{34}$$

A similar argument shows that the two factors appearing in the right side of formula (34) are coprime integers and of order of appearance $k(\ell+1)/2$ and $k(\ell-1)$, respectively. Hence, formula (32) holds, concluding the proof.

6 The Proof of Theorem 3

Let $P(N)$ be the largest prime factor of N with the convention that $P(1)=1$. For $2\le y\le z$, we put

$$\Psi(x;y):=\{N\le x : P(N)\le y\}.$$

Numbers N with $P(N)\le y$ are called *y–smooth numbers*. One of our main tools is the estimate

$$\Psi(t;t^{1/v})=\frac{t}{\exp((1+o(1))v\log v)}\quad \text{whenever}\quad t^{1/v}>(\log t)^2 \tag{35}$$

(see [1]). Here, by $o(1)$ we mean that v tends to infinity, and also t together with it by the inequality in the right–hand side of (35). We only present the argument for $c=1$, since the argument for the general case follows by typographic changes.

We let x be large. We let $u:=u(x)$ be some function of x which tends to infinity with x to be made more precise later. We put $y:=x^{1/u}$.

We let

$$\mathcal{A}_1(x):=\{N\le x : P(N)\le y\}. \tag{36}$$

By estimate (35), we have

$$\#\mathcal{A}_1(x)\le \Psi(x;x^{1/u})=\frac{x}{\exp((1+o(1))u\log u)}\quad \text{as}\quad u\to\infty, \tag{37}$$

where we need to assume that

$$u \leq \frac{\log x}{2 \log \log x}, \tag{38}$$

which we do.

From now on, we assume $N \notin \mathcal{A}_1(x)$. Thus, $N = Pa$ with some prime $P > y$.

Let $\mathcal{P} := \{p : z(p) < p^{1/3}\}$. Let us find an upper bound for $\#\mathcal{P}(t)$. Say t is large and let $\mathcal{P}(t) = \{p_1, \ldots, p_s\}$. Then

$$2^{\#\mathcal{P}(t)} \leq p_1 \cdots p_s \leq \prod_{m < t^{1/3}} F_m < \alpha^{\sum_{m<t^{1/3}} m} < \alpha^{t^{2/3}} < 2^{t^{2/3}}.$$

Here, we used the fact that $F_k < \alpha^k$ for all $k \geq 1$. Thus,

$$\#\mathcal{P}(t) < t^{2/3}. \tag{39}$$

Let

$$\mathcal{A}_2(x) := \{N \leq x \ : N = Pa,\ P > y \text{ but } P \in \mathcal{P}\}. \tag{40}$$

Assume that $N = Pa \in \mathcal{A}_2(x)$, where $P > y$ is in $\mathcal{P}$. Fix a. Observe that $a \leq x/P < x/y$. Then $P < x/a$ is an element in $\mathcal{P}(x/a)$, a set with at most $(x/a)^{2/3}$ elements by estimate (39). Hence,

$$\#\mathcal{A}_2(x) \leq \sum_{a<x/y} \left(\frac{x}{a}\right)^{2/3} \ll x^{2/3} \int_1^{x/y} \frac{dt}{t^{2/3}} \ll \frac{x}{y^{1/3}}. \tag{41}$$

From now on, we assume that $N \notin \mathcal{A}_1(x) \cup \mathcal{A}_2(x)$. Thus, whenever $N = Pa$ with $P > y$, then $z(P) > P^{1/3} > y^{1/3}$.

Put $z := y^{1/(3u)} = x^{1/(3u^2)}$ and let

$$\mathcal{A}_3(x) := \{N \leq x \ : \ N = Pa,\ P > y \text{ and } P(z(P)) \leq z\}. \tag{42}$$

Assume that $N \in \mathcal{A}_3(x)$. Write again $N = Pa$ with $P > y$ and let $d := z(P)$. Then for large x, P is also large, in particular larger than 5, and so the congruence $P \equiv \pm 1 \pmod{d}$ holds. The sign is $+1$ or -1 according to whether P is congruent to $\pm 1 \pmod 5$ or $\pm 2 \pmod 5$, respectively. Fixing

P, the number a can be chosen in at most x/P ways. We now fix d and sum up the above bound over the primes $P \le x$ which are congruent to $\pm 1 \pmod d$, obtaining a contribution of at most

$$\sum_{\substack{P\le x\\ P\equiv \pm 1 \pmod d}} \frac{x}{P} \ll \frac{x\log\log x}{\phi(d)} \ll \frac{x(\log\log x)^2}{d}, \tag{43}$$

where in the above estimates we used the Brun–Titchmarsch theorem concerning the number of primes $P \le x$ in the arithmetic progressions ± 1 modulo d, as well as the minimal order $\phi(d)/d \gg 1/(\log\log x)$ of the Euler function $\phi(d)$ in the interval $[1, x]$. Now we sum up the bounds from inequality (43) over all the d's observing that for our N we have $d > y^{1/3}$ and $P(d) \le z \le d^{1/u}$. Thus, by the Abel summation formula and inequalities (43), we get

$$\begin{aligned} \#\mathcal{A}_3(x) &< x(\log\log x)^2 \sum_{\substack{y^{1/3}\le d\le x\\ P(d)\le d^{1/u}}} \frac{1}{d} \ll x(\log\log x)^2 \int_{y^{1/3}}^{x} \frac{d\Psi(t,t^{1/u})}{t} \\ &\ll x(\log\log x)^2 \left(\frac{\Psi(x,x^{1/u})}{x} + \int_{y^{1/3}}^{x} \frac{\Psi(t,t^{1/u})}{t^2}dt\right). \end{aligned} \tag{44}$$

We assume that the following inequality

$$y^{1/(3u)} > (\log y)^2$$

holds, which is equivalent to

$$\frac{\log x}{3u^2} > 2\log\log x - 2\log u - \log 3. \tag{45}$$

Then estimates (35) hold for $t \in [y^{1/3}, x]$, and inserting them into estimate (44) gives

$$\begin{aligned} \#\mathcal{A}_3(x) &\ll \frac{x(\log\log x)^2}{\exp((1+o(1))u\log u)} \left(1 + \int_{y^{1/3}}^{x} \frac{dt}{t}\right) \\ &\ll \frac{x(\log x)(\log\log x)^2}{\exp((1+o(1))u\log u)} = \frac{x}{\exp((1+o(1))u\log u)} \end{aligned} \tag{46}$$

as $x \to \infty$, where the last estimate holds provided that

$$\log\log x = o(u) \quad \text{as} \quad x \to \infty, \tag{47}$$

which we assume. From now on, we assume that $N \notin \mathcal{A}_1(x) \cup \mathcal{A}_2(x) \cup \mathcal{A}_3(x)$.

Suppose that $N \in \mathcal{N}_1(x)$. Write $N = Pa$ where $P > y$ and $z(P) > z$. There exists a prime number $q > z$ such that $q \mid z(P) \mid z(N) = z(N+1)$. Thus, either $q^2 \mid N+1$, or there is a prime $Q \mid N+1$ such that $q \mid z(Q)$.

Let

$$\mathcal{A}_4(x) := \{N \le x \ : \ q^2 \mid N+1 \text{ for some } q > z\}. \tag{48}$$

Fixing q, the number of $N \le x$ such that $q^2 \mid N+1$ is $\lfloor (x+1)/q^2 \rfloor \le 2x/q^2$. Summing up these bounds over all such q, we get

$$\#\mathcal{A}_4(x) \le \sum_{z<q} \frac{2x}{q^2} \ll x \int_z^\infty \frac{dt}{t^2} \ll \frac{x}{z}. \tag{49}$$

From now on, $N \in \mathcal{N}_1(x) \backslash (\mathcal{A}_1(x) \cup \mathcal{A}_2(x) \cup \mathcal{A}_3(x) \cup \mathcal{A}_4(x))$. Then $N = Pa$ and $N+1 = Qb$, where both $z(P)$ and $z(Q)$ are multiples of a prime $q > z$.

Let

$$\mathcal{A}_5(x) := \{N \le x \ : \ N = Pa, \ \gcd(z(P), a) \text{ is divisible by a prime } q > z\}. \tag{50}$$

Fix P and q. Then the number of $N \le x$ divisible by Pq is $\lfloor x/(Pq) \rfloor \le x/Pq$. We now sum up over all primes P such that $P \equiv \pm 1 \pmod q$, and then over all the primes $q > z$, obtaining that

$$\begin{aligned}
\#\mathcal{A}_5(x) &\le \sum_{q>z} \sum_{\substack{P \le x \\ P \equiv \pm 1 \pmod q}} \frac{x}{Pq} = x \sum_{q>z} \frac{1}{q} \sum_{\substack{P \le x \\ P \equiv \pm 1 \pmod q}} \frac{1}{P} \\
&\ll x \sum_{q>z} \frac{\log\log x}{q\phi(q)} \ll x(\log\log x) \sum_{q>z} \frac{1}{q^2} \ll x(\log\log x) \int_z^\infty \frac{dt}{t^2} \\
&\ll \frac{x \log\log x}{z}.
\end{aligned} \tag{51}$$

In the above estimates, we used again the Brun–Titchmarsch estimate concerning the number of primes $P \le x$ in the arithmetic progressions ± 1 modulo d. From now on, we assume that neither N nor $N+1$ belong to $\mathcal{A}_5(x)$. Thus, for us, q is coprime to ab.

We now look at various possibilities among P, Q, a and b.

Let

$$\#\mathcal{A}_6(x) := \left\{N \in \mathcal{N}_1(x) \backslash \left(\cup_{i=1}^{5} \mathcal{A}_i(x)\right) \ : \ PQ < xz^{1/2}\right\}. \tag{52}$$

Fixing P and Q, N is determined by the congruences

$$N \equiv 0 \pmod{P} \qquad \text{and} \qquad N \equiv -1 \pmod{Q}.$$

The number of such solutions $N \le x$ is at most $x/PQ + 1 \le 2xz^{1/2}/PQ$. Summing this bound up over all pairs of primes (P, Q) such that $P \equiv \pm 1 \pmod{q}$ and $Q \equiv \pm 1 \pmod{q}$ for some prime $q > z$, and then over all the primes $q > z$, we get

$$\begin{aligned} \#\mathcal{A}_6(x) &\le \sum_{q>z} \sum_{\substack{P \le x,\ Q \le x \\ P \equiv \pm 1 \pmod{q} \\ Q \equiv \pm 1 \pmod{q}}} \frac{2xz^{1/2}}{PQ} \ll xz^{1/2} \sum_{q>z} \left(\sum_{\substack{P \le x \\ P \equiv \pm 1 \pmod{q}}} \frac{1}{P} \right)^2 \\ &\ll xz^{1/2} \sum_{q>z} \frac{(\log\log x)^2}{\phi(q)^2} \ll x(\log\log x)^2 z^{1/2} \sum_{q>z} \frac{1}{q^2} \\ &\ll \frac{x(\log\log x)^2}{z^{1/2}}. \end{aligned} \tag{53}$$

From now on, we assume that $N \notin \cup_{i=1}^{6} \mathcal{A}_i(x)$. Thus, since $N(N+1) \le x(x+1) < 2x^2$ but $PQ \ge xz^{1/2}$, it follows that $ab < 2x/z^{1/2}$. Let (u_0, v_0) be the solution (u, v) in positive integers with u minimal of the linear equation

$$ua - vb = -1.$$

We then have that $P = u_0 + bt$ and $Q = v_0 + at$ for some nonnegative integer $t \le x/ab$. Put $P \equiv \varepsilon \pmod{q}$ and $Q \equiv \eta \pmod{q}$, where $\varepsilon,\ \eta \in \{\pm 1\}$. Reducing relation $aP - bQ = -1$ modulo q, we get

$$\varepsilon a - \eta b + 1 \equiv 0 \pmod{q}.$$

The above relation is meaningful in the sense that it signals q as a divisor of $\varepsilon a - \eta b + 1$ only when this expression is not zero. So, let us put

$$\#\mathcal{A}_7(x) := \{N \in \mathcal{N}_1(x) \backslash \left(\cup_{i=1}^{6} \mathcal{A}_i(x)\right) \ : \ \varepsilon a - \eta b + 1 \ne 0\}. \tag{54}$$

To bound the cardinality of $\mathcal{A}_7(x)$, let us look at the triples (a, b, q). Observe that since q does not divide b, we have that $P = u_0 + bt \equiv \varepsilon \pmod{q}$, which leads to $t \equiv (\varepsilon - u_0)b^{-1} \pmod q$. Thus, $t \le x/(ab)$ is in a certain arithmetic progression modulo q. The number of such choices is at most 1 if $qab > x$, and at most $2x/(qab)$ if $qab \le x$. Well, fixing the pair (a,b), q is a prime factor of some nonzero expression of the form $\varepsilon a - \eta b + 1$ for $\varepsilon,\ \eta \in \{\pm 1\}$, therefore there are at most $O(\log x)$ choices for q. Since $ab < 2x/z^{1/2}$, it follows that the number of pairs (a,b) is $\sum_{m\le 2x/z^{1/2}} \tau(m)$, where $\tau(\bullet)$ is the number of divisors function. Thus, in the case $qab > x$, a set of possibilities which we denote by $\mathcal{A}_{7,1}(x)$, the number of such possibilities is at most

$$\#\mathcal{A}_{7,1}(x) \ll \log x \sum_{m\le 2x/z^{1/2}} \tau(m) \ll \frac{x(\log x)^2}{z^{1/2}}. \tag{55}$$

In case $qab \le x$, the set of possibilities which we denote by $\mathcal{A}_{7,2}(x)$, then for a fixed pair (a,b), the number of possibilities is $\le 2x/(qab)$. Now $q > z$ and there are $O(\log x)$ choices for q, so summing up over the possibilities for q when the pair (a,b) is fixed, we get a contribution of $O(x(\log x)/(zab))$. Summing this up over all possible pairs (a,b), we get that the number of possibilities of this type is at most

$$\#\mathcal{A}_{7,2}(x) \ll \frac{x\log x}{z} \sum_{m\le x} \frac{\tau(m)}{m} \ll \frac{x(\log x)^3}{z}. \tag{56}$$

Summing up inequalities (55) and (56), we get

$$\#\mathcal{A}_7(x) \le \#\mathcal{A}_{7,1}(x) + \#\mathcal{A}_{7,2}(x) \ll \frac{x(\log x)^3}{z^{1/2}}. \tag{57}$$

We now look at the N's that are left. Then $\varepsilon a - \eta b = -1$, so $\varepsilon = \eta$ and $b = a + \varepsilon$. Then $N \equiv 0 \pmod a$ and $N \equiv -1 \pmod{a+\varepsilon}$. The number of possibilities for such $N \le x$ is at most $x/(a(a+\varepsilon)) + 1 \le 2x/(a(a+\varepsilon))$, where the last inequality follows because $ab = a(a+\varepsilon) < 2x/z^{1/2} < x$. In the above, and in what follows, we need to assume that $a \ge 2$ when $\varepsilon = -1$. Thus, putting

$$\#\mathcal{A}_8(x) := \{N \in \mathcal{N}_1(x) \backslash \left(\cup_{i=1}^{7} \mathcal{A}_i(x)\right) \ :\ a > z^{1/2}\}, \tag{58}$$

we have that

$$\#\mathcal{A}_8(x) \le \sum_{\varepsilon\in\{1,2\}} \sum_{a>z^{1/2}} \frac{x}{a(a+\varepsilon)} \ll x \sum_{a>z^{1/2}} \frac{1}{a^2} \ll x\int_{z^{1/2}}^{\infty} \frac{dt}{t^2} \ll \frac{x}{z^{1/2}}. \tag{59}$$

Let $\mathcal{A}_9(x)$ be the set of the remaining N. We have $(u_0, v_0) = (\varepsilon, \varepsilon)$. Thus, we need to count the number of $t \le x/(a(a+\varepsilon))$ such that

$$P = \varepsilon + (a+\varepsilon)t \qquad \text{and} \qquad Q = \varepsilon + at$$

are simultaneously prime for $\varepsilon \in \{\pm 1\}$. By the Brun–sieve, for fixed a, the number of such possibilities is at most

$$\begin{aligned} &\ll \sum_{\varepsilon \in \{\pm 1\}} \left(\frac{1}{a(a+\varepsilon)}\right) \frac{x}{(\log(x/(a(a+\varepsilon))))^2} \left(\frac{a(a+\varepsilon)}{\phi(a(a+\varepsilon))}\right)^2 \\ &\ll \frac{x(\log\log(a+2))^2}{a^2(\log x)^2}, \end{aligned} \tag{60}$$

where in the above we used the minimal order $\phi(d)/d \gg 1/\log\log(d+2)$ for all $d \ge 1$ of the Euler function $\phi(d)$, as well as the fact $x/(a(a+\varepsilon)) > x^{1/3}$, which follows for large x because $a + 1 < 2z < x^{1/3}$ (note that u tends to infinity). Summing up over all possible values of a, we get that

$$\#\mathcal{A}_9(x) \ll \frac{x}{(\log x)^2} \sum_{a \ge 1} \frac{(\log\log(a+2))^2}{a^2} \ll \frac{x}{(\log x)^2}. \tag{61}$$

To optimize our arguments, we choose u such that

$$\log(z^{1/2}) = u \log u.$$

With this choice, we get $(1/6)\log x = u^3 \log u$, which we solve and get

$$u = (c_3 + o(1)) \left(\frac{\log x}{\log\log x}\right)^{1/3}, \qquad \text{as} \quad x \to \infty,$$

where $c_3 := 2^{-1/3}$. With this choice, the inequalities (38), (45) and (47) are satisfied, and the upper bounds (37) (41), (46), (49), (51), (53), (57) and (59) give that

$$\#\left(\bigcup_{i=1}^{8} \mathcal{A}_i(x)\right) \le \frac{x}{\exp((c_4 + o(1))(\log x)^{1/3}(\log\log x)^{2/3})} \quad \text{as} \quad x \to \infty, \tag{62}$$

where $c_4 := c_3/3$. Using also (61), we get that

$$\#\mathcal{N}_1(x) \ll \frac{x}{(\log x)^2}. \tag{63}$$

7 Comments

Regarding Theorem 3, its proof shows that we have achieved more than we needed. Our argument separates the members of $\mathcal{N}_1$ into two categories: we say $N \in \mathcal{N}_1$ is *regular* if it is of the form Pa with P prime, $N+1 = Qb$ with Q prime, and a, b are consecutive integers. Otherwise we say $N \in \mathcal{N}_1$ is *special*. We showed in (62) that the number of special values of $N \in \mathcal{N}_1(x)$ is at most

$$x \exp\left(-(c_4 + o(1))(\log x)^{1/3}(\log\log x)^{2/3}\right) \quad \text{as} \quad x \to \infty,$$

and in (63) we showed that the number of regular values of $N \in \mathcal{N}_1(x)$ is $O(x/(\log x)^2)$. This type of separation into two types of solutions might be compared with [4], where the equation $\phi(N) = \phi(N+c)$ is considered.

As in [4] we believe our estimation of $O(x/(\log x)^2)$ for $\#\mathcal{N}_1(x)$ has a matching lower bound of the same magnitude. Here is our heuristic argument for this assertion. Consider the case $a = 1, b = 2$, so that $N = P$ is a regular member of $\mathcal{N}_1$ and $N + 1 = 2Q$. Then

$$P = 2Q - 1.$$

Choose

$$Q \equiv 1 \pmod{10}, \quad Q \equiv 1 \pmod{3}, \quad Q \not\equiv 1 \pmod{9}.$$

Then $z(P) \mid P - 1$, $z(Q) \mid Q - 1$. Assume that

$$z(P) = \frac{P-1}{2} \qquad \text{and} \qquad z(Q) = \frac{Q-1}{3}.$$

Then

$$z(N) = z(P) = \frac{P-1}{2},$$

and

$$z(N+1) = z(2Q) = \operatorname{lcm}[z(2), z(Q)] = \operatorname{lcm}\left[3, \frac{Q-1}{3}\right] = Q - 1 = \frac{P-1}{2}.$$

Hence, if all the above conditions are fulfilled, then indeed we get a solution to $z(N) = z(N+1)$. The Bateman–Horn conjectures imply that there should be $(c_5+o(1))x/(\log x)^2$ primes $Q \le x$ such that $P = 2Q-1$ is also prime as $x \to \infty$, where c_5 is some positive constant. The Extended Riemann-Hypothesis together with the Chebotarev Density Theorem yield that there should be a positive proportion of primes $P \equiv 1 \pmod{10}$ such that $z(P) = (P-1)/2$, and also a positive proportion of primes $Q \equiv 1 \pmod{30}$, but $Q \not\equiv 1 \pmod 9$, such that $z(Q) = (Q-1)/3$. Thus, it could be the fact that for large x there are at least $c_6 x/(\log x)^2$ pairs of primes (P, Q) fulfilling all the above conditions, where c_6 is some positive constant, suggesting that in fact $\#\mathcal{N}_1(x)$ is of order $x/(\log x)^2$. A search up to 10^6, revealed 10 primes P with the above properties namely

$$90121,\ 223441,\ 329761,\ 494761,\ 583801,\ 649801,\ 692521,\ 950161,\ 990841, 996601.$$

If the number of solutions is of order $x/(\log x)^2$ we might expect about 65 new solutions to 10^7, and in fact we found more than this, namely 85 new solutions. This seems to support the heuristic that the number of such examples should be proportional to $x/(\log x)^2$ as x tends to infinity.

Acknowledgments. We thank the referee for comments which improved the quality of the paper and Professor Arnold Knopfmacher for computing the primes $p < 10^7$ mentioned in the last section of the paper. This paper was written while F. L. was on sabbatical from the Mathematical Institute UNAM from January 1 to June 30, 2011 and supported by a PASPA fellowship from DGAPA. C. P. acknowledges support from NSF grant DMS-1001180.

References

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

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

[3] P. Corvaja and U. Zannier, "A lower bound for the height of a rational function at $\mathcal{S}$-unit points", *Monatsh. Math.* **144** (2005), 203–224.

[4] S. W. Graham, J. J. Holt, and C. Pomerance, "On the solutions to $\phi(n) = \phi(n + k)$", in *Number Theory in Progress*, K. Győry, H. Iwaniec, and J. Urbanowicz, eds. vol. 2, de Gruyter, Berlin and New York, 1999, pp. 867–882.

[5] J. S. Han, H. S. Kim and J. Neggers, "The Fibonacci-norm of a positive integer: observations and conjectures", *Int. J. Number Theory* **6** (2010), 371–385.

[6] D. Marques, "On integer numbers with locally smallest order of appearance in the Fibonacci sequence", *Int. J. Math. Math. Sci.* 2011, Art. ID 407643, 4 pp.

[7] E. M. Matveev, "An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II", *Izv. Ross. Akad. Nauk Ser. Mat.* **64** (2000), 125–180; English transl. in *Izv. Math.* **64** (2000), 1217–1269.