DISTRIBUTION OF FIBONACCI AND LUCAS NUMBERS MODULO 3^k

RALF BUNDSCHUH AND PETER BUNDSCHUH

Dedicated to Peter Shiue on the occasion of his 70th birthday

Abstract. Let $F_0 = 0, F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$ denote the sequence $\mathcal{F}$ of Fibonacci numbers. For any modulus $m \geq 2$ and residue $b \pmod m$, denote by $v_{\mathcal{F}}(m, b)$ the number of occurrences of b as a residue in one (shortest) period of $\mathcal{F}$ modulo m. Moreover, let $v_{\mathcal{L}}(m, b)$ be similarly defined for the Lucas sequence $\mathcal{L}$ satisfying $L_0 = 2, L_1 = 1$, and $L_n = L_{n-1} + L_{n-2}$ for $n \geq 2$.

In this paper, completing the recent partial work of Shiu and Chu we entirely describe the functions $v_{\mathcal{F}}(3^k, .)$ and $v_{\mathcal{L}}(3^k, .)$ for every positive integer k. Using a notion formally introduced by Carlip and Jacobson, our main results imply that neither $\mathcal{F}$ nor $\mathcal{L}$ is stable modulo 3. Moreover, in terms of another notion introduced by Somer and Carlip, we observe that $\mathcal{L}$ is a multiple of a translation of $\mathcal{F}$ modulo 3^k (and conversely) for every k.

1. Introduction and results

Wall [11] remarked that second-order linear recurrences $\mathcal{A} = (a_n)_{n=0,1,\ldots}$ of type $a_{n+2} = a_{n+1} + a_n$ $(n \geq 0)$ with arbitrary integer initial values a_0, a_1 are simply periodic if reduced modulo any $m \in \mathbb{N} := \{1, 2, \ldots\}$. He explicitly determined the period length $h_{\mathcal{A}}(m)$ of $\mathcal{A}$ modulo m in terms of a_0, a_1, and m. In particular, his Theorems 5 and 12 imply

$$h_{\mathcal{F}}(3^k) = h_{\mathcal{L}}(3^k) = 8 \cdot 3^{k-1}$$

for any $k \in \mathbb{N}$. Here $\mathcal{F} = (F_n)_{n=0,1,\ldots}$ and $\mathcal{L} = (L_n)_{n=0,1,\ldots}$ denote the sequences of Fibonacci and Lucas numbers defined by

$$F_0 := 0,\ F_1 := 1,\ F_{n+2} := F_{n+1} + F_n \ \ (n \in \mathbb{N}_0), \tag{1.1}$$

$$L_0 := 2,\ L_1 := 1,\ L_{n+2} := L_{n+1} + L_n \ \ (n \in \mathbb{N}_0), \tag{1.2}$$

respectively, where $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$.

In the early 1990s, Jacobson [3] introduced the *frequency distribution function* of $\mathcal{A}$ modulo m

$$v_{\mathcal{A}}(m, b) := \#\{n \,|\, 0 \leq n < h_{\mathcal{A}}(m),\ a_n \equiv b \pmod m\}$$

denoting the number of occurrences of the residue b modulo m in the period of a recurring sequence $\mathcal{A}$ as above. In the same paper, he explicitly described the function $v_{\mathcal{F}}(2^k, b), b \in \{0, \ldots, 2^k - 1\}$, for every $k \in \mathbb{N}$. As a consequence of his description, one can record that the Fibonacci sequence $\mathcal{F}$ is stable modulo 2. The precise definition of stability was given shortly later by Carlip and Jacobson [2], and depends on the image of the distribution function, i.e., on the set

$$\Omega_{\mathcal{A}}(m) := \{v_{\mathcal{A}}(m, b) \,|\, b \in \{0, \ldots, m-1\}\}$$

of all frequencies of residues modulo m in a full period of $\mathcal{A}$ modulo m. In terms of $\Omega_{\mathcal{A}}(m)$, a sequence $\mathcal{A}$ is said to be *stable* modulo a prime p if there is a $k_0 \in \mathbb{N}$ such that $\Omega_{\mathcal{A}}(p^k) = \Omega_{\mathcal{A}}(p^{k_0})$ holds for all integers $k \geq k_0$. As a consequence of Jacobson's main result in [3], one can note $\Omega_{\mathcal{F}}(2^k) = \{0, 1, 2, 3, 8\}$ for every $k \geq 5$, hence the Fibonacci sequence is stable modulo 2. Note also $\Omega_{\mathcal{F}}(5^k) = \{4\}$ for every $k \in \mathbb{N}$, and, more generally, $\Omega_{\mathcal{A}}(m)$ consists of just one element if and only if $\mathcal{A}$ is uniformly distributed modulo m in the sense of Niven [6]. Thus, the concept of stability generalizes the notion of uniform distribution modulo prime powers, and also, by a result of Vélez [10], the notion of f-uniform distribution modulo prime powers.

Very recently, we completely described the function $v_{\mathcal{L}}(p^k, .)$ for $p = 5$ and $p = 2$, see Theorems 1 and 2, respectively, in [1]. As simple consequences we found

$$\Omega_{\mathcal{L}}(5^k) = \{0, 2, 2 \cdot 5, ..., 2 \cdot 5^{[k/2]-1}, 5^{[(k-1)/2]}\}$$

for any $k \geq 2$, and

$$\Omega_{\mathcal{L}}(2^k) = \{0, 1, 2, 3, 2^4, 2^5, ..., 2^{[(k+1)/2]}\}$$

for any $k \geq 9$. Of course, the cases of small k can be easily settled as well. These two results on $\Omega_{\mathcal{L}}$ clearly say that, in contrast to the Fibonacci sequence, the Lucas sequence is neither stable modulo 2 nor modulo 5.

A few years ago, Shiu and Chu started to investigate the function $v_{\mathcal{F}}(3^k, .)$. Whereas they obtained only partial results in this direction, it will be the main aim of the present paper to completely describe $v_{\mathcal{F}}(3^k, .)$ and $v_{\mathcal{L}}(3^k, .)$. Our main results read as follows.

Theorem 1.1. *Suppose that $k \in \mathbb{N}$. Then, for every residue b modulo 3^k, one has*

$$v_{\mathcal{F}}(3^k, b) = \begin{cases} 3^{[k/2]} + 2 & \text{if } b \equiv \pm F_{2 \cdot 3^{2[(k-1)/4]+1}} \pmod{3^k}, \\ 2 \cdot 3^\ell + 2 & \text{if } b \equiv \pm F_{2 \cdot 3^{\ell-1}} \pmod{3^{2\ell+1}} \text{ for some } \ell \in \{1, ..., [(k-1)/2]\}, \\ 2 & \text{otherwise.} \end{cases} \tag{1.3}$$

Theorem 1.2. *Suppose that $k \in \mathbb{N}$. Then, for every residue b modulo 3^k, one has*

$$v_{\mathcal{L}}(3^k, b) = \begin{cases} 3^{[k/2]} + 2 & \text{if } b \equiv \pm L_0 \pmod{3^k}, \\ 2 \cdot 3^\ell + 2 & \text{if } b \equiv \pm L_{4 \cdot 3^{\ell-1}} \pmod{3^{2\ell+1}} \text{ for some } \ell \in \{1, ..., [(k-1)/2]\}, \\ 2 & \text{otherwise.} \end{cases} \tag{1.4}$$

Of course, in both of the above theorems, the case in the second line appears if and only if $k \geq 3$. Moreover, it should be pointed out as a consequence of our proofs that, for every $k \in \mathbb{N}$, for exactly three fourth of the $n \in \{0, ..., 8 \cdot 3^{k-1} - 1\}$, the corresponding F_n belongs to a residue class b modulo 3^k as in the third line of (1.3), i.e., satisfying $v_{\mathcal{F}}(3^k, b) = 2$. On the other hand, the frequency of the n with $F_n \equiv b \pmod{3^k}$, b as in the first line of (1.3), is $O(3^{-k/2})$ hence tends rapidly to zero as $k \to \infty$. The same remarks hold in the Lucas case (with (1.3) replaced by (1.4)).

Clearly, in terms of stability, we can conclude the following from our two main results.

Corollary 1.3. *For every $k \in \mathbb{N}$ and $\mathcal{A} \in \{\mathcal{F}, \mathcal{L}\}$ one has*

$$\Omega_{\mathcal{A}}(3^k) = \{2, 2(3 + 1), 2(3^2 + 1), ..., 2(3^{[(k-1)/2]} + 1), 3^{[k/2]} + 2\},$$

where all but the first and last element have to be omitted if $k \in \{1, 2\}$. Hence neither $\mathcal{F}$ nor $\mathcal{L}$ is stable modulo 3.

This shows that, in contrast to the powers of 2 and 5, the distribution properties of the Fibonacci and Lucas sequences modulo powers of 3 behave very much similar. The deeper reason behind this observation is completely revealed by the fact, to be proved in Lemma 2.5 below, that, *for every $k \in \mathbb{N}$, there exist $c(k), m(k) \in \mathbb{Z}$ with $3 \nmid c(k)$ such that*

$$L_n \equiv c(k) F_{n+m(k)} \pmod{3^k} \tag{1.5}$$

holds for any $n \in \mathbb{Z}$. In terms of Definition 2.3 of Somer and Carlip [9], this means that $\mathcal{L}$ is a *multiple of a translation* of $\mathcal{F}$ modulo 3^k (and conversely). A consequence of this fact, proved in [9] in a much more general setting, is that $\mathcal{F}$ and $\mathcal{L}$ have in their common shortest period the same *pattern* of frequencies of residues whence again $\Omega_{\mathcal{L}}(3^k) = \Omega_{\mathcal{F}}(3^k)$ for every $k \in \mathbb{N}$ (see our Corollary 1.3).

But even if our proof of Lemma 2.5 effectively determines the constants $c(k), m(k)$ in (1.5), it is not at all evident how to simply translate the complete information contained in, say, Theorem 1.1 into that of Theorem 1.2. Of course, the main obstacle here is the appearance of the multiplier $c(k)$ in formula (1.5): It results in a given ordering $\{b_1, b_2, ..., b_{3^k}\}$ of the distinct residues modulo 3^k being translated into another one, $\{c(k)\, b_1, c(k)\, b_2, ..., c(k)\, b_{3^k}\}$, where the control on the position of the individual is lost.

As a side note, the paper [9] exhibits several classes of recurrences of the more general type $a_{n+2} = \sigma a_{n+1} + \tau a_n\, (n \in \mathbb{N}_0)$ failing to be stable modulo a prime p, and provides sufficient criteria for such recurrences to be p-stable. For example, the first part of Theorem 3.5 predicts that neither $\mathcal{F}$ nor $\mathcal{L}$ is stable modulo 3.

To conclude the introduction, we want to discuss briefly the principal results of Shiu and Chu on $v_{\mathcal{F}}(3^k, .)$. The main information of [7], contained in Theorems 4.6 and 4.7, is listed as follows.

Corollary 1.4. *For every* $k \in \mathbb{N}, k \geq 3$, *the following assertions hold.*

$$v_{\mathcal{F}}(3^k, b) = 8 \quad \text{if} \quad b \equiv \pm 1 \pmod{27}, \tag{1.6}$$

$$v_{\mathcal{F}}(3^k, b) = 2 \quad \text{if} \quad b \not\equiv \pm 1, \pm 8 \pmod{27}. \tag{1.7}$$

Namely, to get (1.6) we apply the second line of (1.3) with $\ell = 1$, and notice $F_2 = 1$, by (1.1). To verify (1.7), we note that the hypothesis $b \not\equiv \pm 1, \pm 8 \pmod{27}$ implies $b \not\equiv \pm F_{2\cdot 3^j} \pmod{27}$ for every $j \in \mathbb{N}_0$, by Lemma 2.6 and again $F_2 = 1$. Thus, the cases in the first two lines of (1.3) cannot occur since all moduli appearing there are at least third powers of 3.

The main result of [8] is the following consequence of our Theorem 1.1.

Corollary 1.5. *For* $k \in \mathbb{N}, k \geq 5$, *and* $b \equiv \pm 8 \pmod{243}$, *one has* $v_{\mathcal{F}}(3^k, b) = 20$.

Namely, since $k \geq 5$ we may apply the result in the second line of (1.3) with $\ell = 2$, and $b \equiv \pm 8 \pmod{243}$ says exactly $b \equiv \pm F_{2\cdot 3^2 - 1} \pmod{3^{2\cdot 2+1}}$.

2. Some general lemmas on Fibonacci and Lucas numbers

First, we recall the well-known Binet formulae

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad L_n = \alpha^n + \beta^n \tag{2.1}$$

for the Fibonacci and Lucas numbers, respectively, where $\alpha := (1 + \sqrt{5})/2$, $\beta := (1 - \sqrt{5})/2$. They are easily proved to be valid for every $n \in \mathbb{N}_0$ (see, e.g., Theorems 5.6 and 5.8 of the monograph [5]) but one can use (2.1) to *define* these numbers also for negative integers n. From $\alpha\beta = -1$ the formulae $F_{-n} = (-1)^{n+1} F_n, L_{-n} = (-1)^n L_n$ for any $n \in \mathbb{Z}$ are obvious, and this explains why restriction to nonnegative subscripts of F or L is unnecessary when discussing their divisibility properties.

Our first lemma collects some well-known facts on Fibonacci and Lucas numbers.

Lemma 2.1. *The following statements hold for any $n \in \mathbb{Z}$.*

$$F_{2n} = F_n L_n, \tag{2.2}$$
$$L_{2n} = L_n^2 - 2(-1)^n, \tag{2.3}$$
$$L_{2n} = F_n L_{n+1} + F_{n-1} L_n, \tag{2.4}$$
$$F_{3n} = F_n(5F_n^2 + 3(-1)^n), \tag{2.5}$$
$$L_{3n} = L_n(L_n^2 - 3(-1)^n). \tag{2.6}$$

If (a, b) denotes the greatest common divisor of $a, b \in \mathbb{Z}$, not both zero, then

$$(F_{qn+r}, F_n) = (F_n, F_r) \tag{2.7}$$

holds for any $n, q, r \in \mathbb{Z}$ with n, r not both zero.

Proof. For (2.7), we refer to Lemma 16.2 in [5]. For the simpler items (2.2) through (2.6), the reader is recommended to find his or her own proofs solely on the basis of (2.1). □

Our next auxiliary result expresses differences of two Fibonacci or Lucas numbers as products of such numbers.

Lemma 2.2. *For all $s, t \in \mathbb{Z}$ of the same parity, the following alternatives hold.*

$$F_s - F_t = \begin{cases} F_{(s-t)/2} L_{(s+t)/2} & \text{if } 4 \mid (s-t), \\ F_{(s+t)/2} L_{(s-t)/2} & \text{if } 2 \parallel (s-t), \end{cases} \tag{2.8}$$

$$L_s - L_t = \begin{cases} 5F_{(s+t)/2} F_{(s-t)/2} & \text{if } 4 \mid (s-t), \\ L_{(s+t)/2} L_{(s-t)/2} & \text{if } 2 \parallel (s-t). \end{cases} \tag{2.9}$$

Proof. To establish (2.8), we follow our proof of (2.9) in [1]. With $q := (s+t)/2, r := (s-t)/2 \;\Leftrightarrow\; s = q + r, t = q - r$ we obtain from (2.1) and $\alpha\beta = -1$

$$\begin{aligned} \sqrt{5}(F_s - F_t) = \sqrt{5}(F_{q+r} - F_{q-r}) &= (\alpha^{q+r} - \alpha^{q-r}) - (\beta^{q+r} - \beta^{q-r}) \\ &= \alpha^q(\alpha^r - \varepsilon_r \beta^r) - \beta^q(\beta^r - \varepsilon_r \alpha^r) \\ &= (\alpha^q + \varepsilon_r \beta^q)(\alpha^r - \varepsilon_r \beta^r). \end{aligned}$$

Since $\varepsilon_r := (-1)^r$ we have (2.8). □

The formulae (2.8) and (2.9) will play a decisive role when considering congruences of two Fibonacci or Lucas numbers modulo powers of a prime p on condition that we can calculate or estimate the multiplicities of p in the single factors on the right-hand sides of (2.8) and (2.9).

To state the corresponding results conveniently, we first give the following definition (see [4]). For $z \in \mathbb{Z}\backslash\{0\}$, let $t \in \mathbb{N}_0$ be defined by the divisibility properties[1] $p^t \mid z$, $p^{t+1} \nmid z$. Then we write $\mathrm{ord}_p z$ for this t and call it the *p-order of z*. It is obvious that, using this notation, we can write congruences $z_1 \equiv z_2 \pmod{p^k}$ equivalently as $\mathrm{ord}_p(z_1 - z_2) \geq k$ for $z_1, z_2 \in \mathbb{Z}$ with the extra convention $\mathrm{ord}_p 0 := +\infty$. Main rules on the p-order as $\mathrm{ord}_p(z_1 z_2) = \mathrm{ord}_p z_1 + \mathrm{ord}_p z_2$, or $\mathrm{ord}_p(z_1 + z_2) \geq \min(\mathrm{ord}_p z_1, \mathrm{ord}_p z_2)$, the latter with equality if $\mathrm{ord}_p z_1 \neq \mathrm{ord}_p z_2$, are easily checked.

[1] Clearly, this means the same as the usual notation $p^t \| z$ used, e.g., in Lemma 2.2.

Lemma 2.3. *For $n \in \mathbb{Z}$, the following assertions hold, $n = 0$ being excluded in the last two items.*

$$4 \mid n \quad \Leftrightarrow \quad 3 \mid F_n, \tag{2.10}$$
$$4 \mid n \quad \Rightarrow \quad \mathrm{ord}_3\, F_n = 1 + \mathrm{ord}_3\, n, \tag{2.11}$$
$$2 \parallel n \quad \Leftrightarrow \quad 3 \mid L_n, \tag{2.12}$$
$$2 \parallel n \quad \Rightarrow \quad \mathrm{ord}_3\, L_n = 1 + \mathrm{ord}_3\, n. \tag{2.13}$$

Proof. (2.10) and (2.12) are obvious since $\mathcal{F}$ and $\mathcal{L}$ have period length 8 modulo 3, begin with 0,1,1,2,0,2,2,1 and 2,1,0,1,1,2,0,2, respectively, and then repeat.

Assuming $n \neq 0$ we use for (2.11) (and for (2.13)) induction on $\mathrm{ord}_3\, n \in \mathbb{N}_0$. Let $4 \mid n, 3 \nmid n$ hence $n \equiv \pm 4 \pmod{12}$, or equivalently, $n = 12j \pm 4$ with some $j \in \mathbb{Z}$. By $F_{\pm 4} = \pm 3, 18 = L_6 \mid F_{12}$ (compare (2.2)) and (2.7), we have $(F_{12j\pm 4}, F_{12}) = (F_{12}, F_{\pm 4}) = 3$ for the greatest common divisors, whence $\mathrm{ord}_3\, F_n = 1$. This proves (2.11) for $\mathrm{ord}_3\, n = 0$. Suppose now that (2.11) is already proved for $u := \mathrm{ord}_3\, n \in \mathbb{N}_0$, i.e., if $n = 4 \cdot 3^u v$ with $3 \nmid v$. Then we find from (2.5)

$$\mathrm{ord}_3\, F_{4\cdot 3^{u+1}v} = \mathrm{ord}_3\, F_{4\cdot 3^u v} + \mathrm{ord}_3\, (5F^2_{4\cdot 3^u v} + 3) = \mathrm{ord}_3\, F_{4\cdot 3^u v} + 1,$$

and this is the inductive step.

For (2.13), suppose $2 \parallel n$ and $3 \nmid n$. Then, in $L_n = F_{2n}/F_n$, the denominator is not divisible by 3 but $\mathrm{ord}_3\, F_{2n} = 1 + \mathrm{ord}_3\, (2n) = 1$, by (2.11). Assume that (2.13) is proved for $u = \mathrm{ord}_3\, n \in \mathbb{N}_0$, i.e., if $n = 2 \cdot 3^u v$ with integer v coprime to 6. Then we conclude from (2.6)

$$\mathrm{ord}_3\, L_{2\cdot 3^{u+1}v} = \mathrm{ord}_3\, L_{2\cdot 3^u v} + \mathrm{ord}_3\, (L^2_{2\cdot 3^u v} + 3) = \mathrm{ord}_3\, L_{2\cdot 3^u v} + 1,$$

whence the last assertion of our lemma. □

Lemma 2.4. *For all $k \in \mathbb{N}$ and $n \in \mathbb{Z}$, the following congruences hold.*

$$F_{n+4\cdot 3^{k-1}} \equiv -F_n \pmod{3^k}, \tag{2.14}$$
$$L_{n+4\cdot 3^{k-1}} \equiv -L_n \pmod{3^k}. \tag{2.15}$$

Proof. Because of the recurrence relations (1.1) and (1.2) it is enough to prove both of these congruences for $n = 0$ and $n = 1$.

Concerning (2.14) we note that $F_{4\cdot 3^{k-1}} \equiv 0 \pmod{3^k}$, by (2.11). Since $\mathcal{F}$ has period length $8 \cdot 3^{k-1}$ modulo 3^k, we obtain, by (2.2),

$$3^k \mid (F_{8\cdot 3^{k-1}+2} - F_2) = F_{2(4\cdot 3^{k-1}+1)} - 1 = F_{4\cdot 3^{k-1}+1} L_{4\cdot 3^{k-1}+1} - 1 \equiv -F_{4\cdot 3^{k-1}+1} L_1 - 1$$

anticipating (2.15) for $n = 1$, and the last term equals $-(F_{4\cdot 3^{k-1}+1} + F_1)$.

To obtain (2.15) for $n = 0$, we use (2.3) to get

$$2 = L_0 \equiv L_{8\cdot 3^{k-1}} = L^2_{4\cdot 3^{k-1}} - 2 \pmod{3^k}$$

or equivalently

$$3^k \mid (L_{4\cdot 3^{k-1}} + 2)(L_{4\cdot 3^{k-1}} - 2).$$

Since $2^2 \parallel j \Rightarrow L_j \equiv 1 \pmod 3$, the second factor is not divisible by 3, hence $L_{4\cdot 3^{k-1}} \equiv -2 = -L_0 \pmod{3^k}$, and (2.15) is established for $n = 0$. Using again (2.3), we obtain furthermore

$$3^k \mid (L_{8\cdot 3^{k-1}+2} - L_2) = L^2_{4\cdot 3^{k-1}+1} + 2 - 3 = (L_{4\cdot 3^{k-1}+1} + 1)(L_{4\cdot 3^{k-1}+1} - 1).$$

Since $L_j \equiv 2 \pmod 3$ for $j \equiv 5 \pmod 8$, the second factor on the right-hand side is not divisible by 3, and we have (2.15) for $n = 1$. □

The subsequent lemma is only needed to deduce formula (1.5), even including explicit expressions for $c(k)$ and $m(k)$.

Lemma 2.5. *For every $k \in \mathbb{N}$ and $n \in \mathbb{Z}$, one has the congruence*
$$F_{3^{k-1}} L_n \equiv L_{3^{k-1}} F_{n-2\cdot 3^{k-1}} \pmod{3^k}. \tag{2.16}$$

Proof. Let $k \in \mathbb{N}$ be fixed. We argue by induction on n. Since $F_{-3^{k-1}} = F_{3^{k-1}}$, the congruence (2.16) is satisfied for $n = 3^{k-1}$ (in fact, the congruence reduces then to an equation). Using (2.4) with $n = 3^{k-1}$, we obtain
$$F_{3^{k-1}} L_{3^{k-1}+1} + F_{3^{k-1}-1} L_{3^{k-1}} = L_{2\cdot 3^{k-1}} \equiv 0 \pmod{3^k}$$
taking (2.13) into account. But, by $F_{3^{k-1}-1} = -F_{1-3^{k-1}}$, this is (2.16) for $n = 3^{k-1}+1$. Since (2.16) holds for two successive n's, it holds for all integers n. □

Remark. From (2.16) we see immediately that (1.5) holds with $m(k) = -2\cdot 3^{k-1}$ and $c(k) = L_{3^{k-1}} F_{3^{k-1}}^{-1}$, where $F_{3^{k-1}}^{-1}$ has to be interpreted as the inverse of $F_{3^{k-1}}$ in $\mathbb{Z}_{3^k}^*$, the residue class group modulo 3^k. Note that $F_{3^{k-1}}$ (and $L_{3^{k-1}}$) is not a multiple of 3, by (2.10) (and (2.12)).

Our next and again very special lemma is only needed to deduce (1.7) of Corollary 1.4 from our Theorem 1.1.

Lemma 2.6. *For every $j \in \mathbb{N}$, the following congruence holds*
$$F_{2\cdot 3^j} \equiv 8(-1)^{j-1} \pmod{27}. \tag{2.17}$$

Proof. By induction on j. First, we have $F_6 = 8$. Assuming that (2.17) holds, we use (2.5) with $n = 2\cdot 3^j$ to obtain modulo 27
$$F_{2\cdot 3^{j+1}} = F_{2\cdot 3^j}(5F_{2\cdot 3^j}^2 + 3) \equiv 8(-1)^{j-1}\cdot 323 = 8(-1)^{j-1}\cdot(12\cdot 27 - 1) \equiv 8(-1)^j,$$
and this yields the inductive step. □

3. More direct preparation of the main proof

The subsequent Proposition 3.2 prepares our proofs of the formulae for $v_{\mathcal{F}}(3^k, b)$ and $v_{\mathcal{L}}(3^k, b)$ in the case of b's as in the first line of (1.3) and (1.4), respectively.

Lemma 3.1. *If $k \in \mathbb{N}$, then the following congruences modulo 3^k hold for any $j \in \mathbb{Z}$.*
$$F_{J(k)+8\cdot 3^{[(k-1)/2]}j} \equiv F_{J(k)} \quad \text{with} \quad J(k) := 2\cdot 3^{2[(k-1)/4]+1}, \tag{3.1}$$
$$L_{8\cdot 3^{[(k-1)/2]}j} \equiv L_0. \tag{3.2}$$

Proof. By (2.8), we obtain
$$F_{J(k)+8\cdot 3^{[(k-1)/2]}j} - F_{J(k)} = F_{4\cdot 3^{[(k-1)/2]}j} L_{J(k)+4\cdot 3^{[(k-1)/2]}j}.$$
Taking here ord_3, and using (2.11) and (2.13), we conclude
$$\mathrm{ord}_3(F_{J(k)+8\cdot 3^{[(k-1)/2]}j} - F_{J(k)}) \geq 2(1 + [(k-1)/2]) \geq k,$$
hence (3.1). Notice here that $2[(k-1)/4] + 1 - [(k-1)/2]$ equals 0 or 1 for every $k \in \mathbb{Z}$. Similarly, by (2.9) and again (2.11) one finds
$$\mathrm{ord}_3(L_{8\cdot 3^{[(k-1)/2]}j} - L_0) = \mathrm{ord}_3(5F_{4\cdot 3^{[(k-1)/2]}j}^2) \geq 2(1 + [(k-1)/2] \geq k,$$
whence (3.2). □

From Lemmas 2.4 and 3.1 we now easily deduce the following.

Proposition 3.2. *If $k\in\mathbb{N}$, then there are at least $3^{[k/2]}$ even $n\in\{0,...,8\cdot 3^{k-1}-1\}$ satisfying*

$$F_n \equiv F_{J(k)} \pmod{3^k} \tag{3.3}$$

with $J(k)$ as defined in (3.1). The same assertion holds for the congruence

$$F_n \equiv -F_{J(k)} \pmod{3^k}, \tag{3.4}$$

and for both of the congruences

$$L_n \equiv \pm L_0 \pmod{3^k}.$$

Proof. For the statement concerning (3.3) it is enough to check that $0 \le J(k)+8\cdot 3^{[(k-1)/2]}j < 8\cdot 3^{k-1}$ holds (exactly) if $0 \le j < 3^{[k/2]}$. The computation is easy and uses $[(k-1)/2]+[k/2] = k-1$ for any integer k.

To obtain our claim concerning (3.4), we use (2.14) from Lemma 2.4, and count the even $n \in \{0,...,8\cdot 3^{k-1}-1\}$ satisfying

$$F_n \equiv F_{J(k)+4\cdot 3^{k-1}} \pmod{3^k}$$

or equivalently, the even $n \in \{4\cdot 3^{k-1},...,12\cdot 3^{k-1}-1\}$ satisfying (3.3).

The proof in the Lucas case on the basis of (3.2) is similar but, to handle $L_n \equiv -L_0 (\mathrm{mod}\ 3^k)$, one applies (2.15). □

We next prepare our proofs of the formulae for $v_{\mathcal{F}}(3^k,b)$ and $v_{\mathcal{L}}(3^k,b)$ in the case of b's as in the second line of (1.3) and (1.4), respectively.

Lemma 3.3. *If $\ell \in \mathbb{N}$, then the following congruences hold*

$$F_n \equiv F_{2\cdot 3^{\ell-1}} \pmod{3^{2\ell+1}} \tag{3.5}$$

if n is either of the form $2\cdot 3^{\ell-1}+8\cdot 3^{\ell}j$, or of the form $10\cdot 3^{\ell-1}+8\cdot 3^{\ell}j$ with some $j\in\mathbb{Z}$.

$$L_n \equiv L_{4\cdot 3^{\ell-1}} \pmod{3^{2\ell+1}} \tag{3.6}$$

if n is either of the form $4\cdot 3^{\ell-1}+8\cdot 3^{\ell}j$, or of the form $-4\cdot 3^{\ell-1}+8\cdot 3^{\ell}j$ with some $j\in\mathbb{Z}$.

Proof. If $i\in\{1,5\}$, then we deduce from (2.8), (2.11), (2.13), and

$$\mathrm{ord}_3(F_{2\cdot 3^{\ell-1}i+8\cdot 3^{\ell}j}-F_{2\cdot 3^{\ell-1}}) = \mathrm{ord}_3(F_{3^{\ell-1}(i-1)+4\cdot 3^{\ell}j}L_{3^{\ell-1}(i+1)+4\cdot 3^{\ell}j}) \ge 2\ell+1,$$

whence (3.5). Note here that, for $i=1$, the first factor on the right-hand side has 3-order at least $\ell+1$ and the second at least ℓ, and for $i=5$ the converse holds.

With $i\in\{1,-1\}$ we obtain from (2.9) and (2.11)

$$\mathrm{ord}_3(L_{4\cdot 3^{\ell-1}i+8\cdot 3^{\ell}j}-L_{4\cdot 3^{\ell-1}}) = \mathrm{ord}_3(5F_{2\cdot 3^{\ell-1}(i-1)+4\cdot 3^{\ell}j}F_{2\cdot 3^{\ell-1}(i+1)+4\cdot 3^{\ell}j}) \ge 2\ell+1$$

considering again both of the cases i separately. Thus, (3.6) holds for all n indicated there. □

From Lemmas 2.4 and 3.3, we easily establish the following counting result.

Proposition 3.4. *If $\ell\in\mathbb{N}$, then there are at least $2\cdot 3^{\ell}$ even $n\in\{0,...,8\cdot 3^{2\ell}-1\}$ satisfying (3.5), and the same assertion holds for the congruence*

$$F_n \equiv -F_{2\cdot 3^{\ell-1}} \pmod{3^{2\ell+1}}, \tag{3.7}$$

and for both of the congruences

$$L_n \equiv \pm L_{4\cdot 3^{\ell-1}} \pmod{3^{2\ell+1}}.$$

Proof. For the assertion on (3.5), we count the number of $n \in \{0, ..., 8 \cdot 3^{k-1} - 1\}$ of the form $2 \cdot 3^{\ell-1} + 8 \cdot 3^{\ell} j$ or $10 \cdot 3^{\ell-1} + 8 \cdot 3^{\ell} j$. As it is easily checked, these are (exactly) those n arising from $j \in \{0, ..., 3^{\ell} - 1\}$. Concerning (3.7) we argue similarly to our counting considerations on (3.4) via (2.14).

The proof in the Lucas case runs on the basis of (3.6) and, one applies (2.15) once more to treat $L_n \equiv -L_{4 \cdot 3^{\ell-1}} (\bmod\ 3^{2\ell+1})$ □

Our last two lemmas concern the b's of the third line of (1.3) and (1.4), and, in case of b's as in the first or second lines, the contribution of odd n's to $v_{\mathcal{F}}(3^k, b)$ or to $v_{\mathcal{L}}(3^k, b)$.

Lemma 3.5. *Let $k \in \mathbb{N}$. If F_n (or L_n) with some $n \in \{0, ..., 8 \cdot 3^{k-1} - 1\}$, $n \not\equiv 2$ (or $n \not\equiv 0$, resp.) $(\bmod\ 4)$ leaves modulo 3^k the remainder $b \in \{0, ..., 3^k - 1\}$, then the $F_{n+8 \cdot 3^{k-1} j}$ (or $L_{n+8 \cdot 3^{k-1} j}$, resp.), $j = 0, 1, 2$, leave modulo 3^{k+1} the remainders $b + 3^k \lambda$ with $\lambda = 0, 1, 2$.*

Proof. Using (2.8) or (2.9), respectively, we have for integers $0 \le i < j \le 2$

$$\begin{aligned} F_{n+8 \cdot 3^{k-1} j} - F_{n+8 \cdot 3^{k-1} i} &= F_{4 \cdot 3^{k-1}(j-i)} L_{n+4 \cdot 3^{k-1}(j+i)}, \\ L_{n+8 \cdot 3^{k-1} j} - L_{n+8 \cdot 3^{k-1} i} &= 5 F_{4 \cdot 3^{k-1}(j-i)} F_{n+4 \cdot 3^{k-1}(j+i)}. \end{aligned}$$

In the first equation, the subscript of L is $\not\equiv 2 \,(\bmod\ 4)$, by our hypothesis on n, whereas, in the second equation, the subscript of the second factor on the right-hand side is $\not\equiv 0 \,(\bmod\ 4)$. Thus, in both of these equations, the factor of $F_{4 \cdot 3^{k-1}(j-i)}$ is not divisible by 3, by (2.10) and (2.12), respectively. Hence we find, by virtue of (2.11),

$$\operatorname{ord}_3(F_{n+8 \cdot 3^{k-1} j} - F_{n+8 \cdot 3^{k-1} i}) = \operatorname{ord}_3(L_{n+8 \cdot 3^{k-1} j} - L_{n+8 \cdot 3^{k-1} i}) = k$$

since $j - i$ is either 1 or 2. Thus, the $F_{n+8 \cdot 3^{k-1} j}$ $(j = 0, 1, 2)$ are pairwise incongruent modulo 3^{k+1}, and the same holds for the $L_{n+8 \cdot 3^{k-1} j}$ $(j = 0, 1, 2)$. Writing $F_{n+8 \cdot 3^{k-1} j} = b + 3^k \lambda_j$ with suitable integers $\lambda_j \,(j = 0, 1, 2)$, we conclude that $\lambda_0, \lambda_1, \lambda_2$ are pairwise incongruent modulo 3, whence our desired result in the Fibonacci case. The argument in the Lucas case is the same. □

Lemma 3.6. *For every residue b modulo 3^k, there are exactly two $n \in \{0, ..., 8 \cdot 3^{k-1} - 1\}$ satisfying*

$$F_n \equiv b \quad (\text{or } L_n \equiv b) \quad \text{modulo } 3^k,$$

provided that, in case of b's as in the first or second line of (1.3) (or (1.4), resp.) only odd n's are counted.

Remark. This implies already

$$v_{\mathcal{F}}(3^k, b) = v_{\mathcal{L}}(3^k, b) = 2$$

for any residue b modulo 3^k occurring in the third line of (1.3) and (1.4).

Proof. The validity of the lemma will be settled by induction on k. For $k = 1$, we have modulo 3

$$F_n \equiv 1 \text{ if } n = 1, 2, 7, \quad F_n \equiv 2 \text{ if } n = 3, 5, 6, \quad F_n \equiv 0 \text{ if } n = 0, 4,$$

or

$$L_n \equiv 1 \text{ if } n = 1, 3, 4, \quad L_n \equiv 2 \text{ if } n = 0, 5, 7, \quad L_n \equiv 0 \text{ if } n = 2, 6,$$

respectively. If $b \equiv 1$ or $b \equiv -1$ (mod 3), then in the Fibonacci case, we have to omit $n = 2$ and $n = 6$, whereas in the Lucas case $n = 4$ and $n = 0$ have to be omitted. After these omissions, in both of the cases, for every possible residue modulo 3, there remain exactly two 'admissible' n-values no one of them being congruent to 2 (or to 0) modulo 4 in the Fibonacci (or Lucas) case. (Note that, for $k = 1$, the second line in (1.3) and (1.4) does not occur, whereas the condition in the first line says precisely $b \equiv \pm 1 \pmod 3$.)

Having these considerations in mind, in both of the cases Fibonacci and Lucas, the inductive step is easily performed via Lemma 3.5. $\square$

4. Final proof

According to Propositions 3.2 and 3.4, the number of even subscripts $n \in \{0, ..., 8 \cdot 3^{k-1} - 1\}$ counted for residues b as in the first and second line of (1.3) or (1.4) is *at least*

$$2 \cdot 3^{[k/2]} + \sum_{\ell=1}^{[(k-1)/2]} (2 \cdot 3^\ell) \cdot 2 \cdot 3^{k-1-2\ell} = 2 \cdot 3^{[k/2]} + 4 \cdot \sum_{\ell=0}^{[(k-1)/2]-1} 3^{k-2-\ell}$$

$$= 2 \cdot 3^{[k/2]} + 4 \cdot 3^{k-2} \, \frac{1 - 3^{-[(k-1)/2]}}{2/3} = 2 \cdot 3^{[k/2]} + 2 \cdot 3^{k-1}(1 - 3^{-[(k-1)/2]}) = 2 \cdot 3^{k-1},$$

where we used again $[(k-1)/2] + [k/2] = k - 1$. Note further that above, in the first sum over ℓ, the complete residue set $\{0, ..., 3^k - 1\}$ modulo 3^k decomposes, for every fixed $\ell \in \{1, ..., [(k-1)/2]\}$, into exactly $3^{k-1-2\ell}$ complete residue systems modulo $3^{2\ell+1}$, a typical representative being $\{0, ..., 3^{2\ell+1} - 1\}$.

Defining

$$v_{\mathcal{F}}^{even}(3^k, b) := \#\{n \,|\, 0 \le n < 8 \cdot 3^{k-1}, 2 \,|\, n, F_n \equiv b \pmod{3^k}\}$$

and similarly $v_{\mathcal{F}}^{odd}$ if condition $2 \,|\, n$ is replaced by $2 \not|\, n$, then our last consideration implies the left-hand part of the following formula

$$2 \cdot 3^{k-1} \le \sum_{b \in I \cup II} v_{\mathcal{F}}^{even}(3^k, b) = 8 \cdot 3^{k-1} - \Big(\sum_{b \in III} v_{\mathcal{F}}(3^k, b) + \sum_{b \in I \cup II} v_{\mathcal{F}}^{odd}(3^k, b) \Big). \tag{4.1}$$

Here $b \in I \cup II$ (or $b \in III$) means that the summation is over all residues b as in the first or second line (or in the third line, respectively) of (1.3), and the same formula holds with $\mathcal{F}$ replaced by $\mathcal{L}$. According to Lemma 3.5, we have

$$v_{\mathcal{F}}^{odd}(3^k, b) = 2 \text{ for any } b \in I \cup II, \quad v_{\mathcal{F}}(3^k, b) = 2 \text{ for any } b \in III,$$

whence the right-hand side of (4.1) equals $8 \cdot 3^{k-1} - 2 \cdot 3^k = 2 \cdot 3^{k-1}$, and this is the left-hand side of (4.1). This means that, in Propositions 3.2 and 3.4, all *at least*'s can be replaced by *exactly*. This implies

$$v_{\mathcal{F}}(3^k, b) = v_{\mathcal{F}}^{even}(3^k, b) + v_{\mathcal{F}}^{odd}(3^k, b) = 3^{[k/2]} + 2$$

for all b as in the first line of (1.3), and

$$v_{\mathcal{F}}(3^k, b) = v_{\mathcal{F}}^{even}(3^k, b) + v_{\mathcal{F}}^{odd}(3^k, b) = 2 \cdot 3^\ell + 2$$

for all b as in the second line of (1.3) for some $\ell \in \{1, ..., [(k-1)/2]\}$. Since our final argument remains unchanged if $\mathcal{F}$ is replaced by $\mathcal{L}$ both of our theorems are proved.

5. An additional comment

One can avoid the previous discussion replacing the inequality in (4.1) by equality as follows. First, we can replace Lemma 3.1 by the subsequent stronger result.

Lemma 3.1*. *For any $k \in \mathbb{N}$, the following two equivalences are valid for any even $n \in \mathbb{Z}$.*

$$F_n \equiv F_{J(k)} \pmod{3^k} \qquad \Leftrightarrow \qquad n \in J(k) + 8 \cdot 3^{[(k-1)/2]}\mathbb{Z},$$
$$L_n \equiv L_0 \pmod{3^k} \qquad \Leftrightarrow \qquad n \in 8 \cdot 3^{[(k-1)/2]}\mathbb{Z}.$$

Note that (3.1) and (3.2) contain just the $\Leftarrow$ part of the two equivalences. Having here the full information $\Leftrightarrow$, we can easily replace *at least* in Proposition 3.2 by *exactly*.

Secondly, we can improve Lemma 3.3 as follows.

Lemma 3.3*. *If $\ell \in \mathbb{N}$, then the following two equivalences are valid for any even $n \in \mathbb{Z}$.*

$$F_n \equiv F_{2\cdot 3^{\ell-1}} \pmod{3^{2\ell+1}} \quad \Leftrightarrow \quad n \in (2 \cdot 3^{\ell-1} + 8 \cdot 3^{\ell}\mathbb{Z}) \cup (10 \cdot 3^{\ell-1} + 8 \cdot 3^{\ell}\mathbb{Z}),$$
$$L_n \equiv L_{4\cdot 3^{\ell-1}} \pmod{3^{2\ell+1}} \quad \Leftrightarrow \quad n \in (4 \cdot 3^{\ell-1} + 8 \cdot 3^{\ell}\mathbb{Z}) \cup (-4 \cdot 3^{\ell-1} + 8 \cdot 3^{\ell}\mathbb{Z}).$$

Note that also (3.5) and (3.6) contain only the part $\Leftarrow$ of the two equivalences. Here also, the full information $\Leftrightarrow$, allows to replace *at least* in Proposition 3.4 by *exactly*.

The attentive reader may have noticed that the second alternatives in (2.8) and (2.9) concerning the case $2 \parallel (s-t)$ have not yet been used until now. These alternatives are needed to discuss the implications $\Rightarrow$ in Lemmas 3.1* and 3.3*. However, this is not the only reason why these latter implications are considerably more delicate to prove.

References

[1] P. Bundschuh and R. Bundschuh, *The sequence of Lucas numbers is not stable modulo* 2 *and* 5, Unif. Distrib. Theory, **5** (2010), 113–130.

[2] W. Carlip and E. T. Jacobson, *Unbounded stability of two-term recurrence sequences modulo* 2^k, Acta Arith., **74** (1996), 329–346.

[3] E. T. Jacobson, *Distribution of the Fibonacci numbers mod* 2^k, The Fibonacci Quarterly, **30** (1992), 211–215.

[4] N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, 2nd ed., Springer, New York et al., 1984.

[5] T. Koshy, *Fibonacci and Lucas numbers with applications*, John Wiley & Sons, Inc., New York et al., 2001.

[6] I. Niven, *Uniform distribution of sequences of integers*, Trans. Amer. Math. Soc., **98** (1961), 52–61.

[7] W. C. Shiu and C. I. Chu, *Distribution of the Fibonacci numbers modulo* 3^k, The Fibonacci Quarterly, **43** (2005), 22–28.

[8] W. C. Shiu and C. I. Chu, *Frequency of Fibonacci numbers modulo* 3^k *that are congruent to* 8(mod 27), Int. J. Pure Appl. Math., **33** (2006), 7–21.

[9] L. Somer and W. Carlip, *Stability of second-order recurrences modulo* p^r, Int. J. Math. Math. Sci., **23** (2000), 225–241.

[10] W. Y. Vélez, *Uniform distribution of two-term recurrence sequences*, Trans. Amer. Math. Soc., **301** (1987), 37–45.

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

AMS Classification Numbers: 11B50, 11B39

Departments of Physics and Biochemistry, The Ohio State University, 191 W Woodruff Av, Columbus, OH 43210, USA

E-mail address: bundschuh@mps.ohio-state.edu

Mathematisches Institut, Universität zu Köln, Weyertal 86-90, D-50931 Köln, Germany

E-mail address: pb@math.uni-koeln.de