THE SEQUENCE OF LUCAS NUMBERS IS NOT STABLE MODULO 2 AND 5

PETER BUNDSCHUH AND RALF BUNDSCHUH

Dedicated to the Memory of Professor Edmund Hlawka

ABSTRACT. Let $L_0 = 2, L_1 = 1$, and $L_n = L_{n-1} + L_{n-2}$ for $n \geq 2$, denote the sequence $\mathcal{L}$ of Lucas numbers. For any modulus $m \geq 2$, and residue $b \,(\mathrm{mod}\, m)$, denote by $v_{\mathcal{L}}(m, b)$ the number of occurrences of b as a residue in one (shortest) period of $\mathcal{L}$ modulo m.

In this paper, we completely describe the functions $v_{\mathcal{L}}(p^k, .)$ for $k \geq 1$ in the cases $p = 2$ and $p = 5$. Using a notion formally introduced by Carlip and Jacobson, our main results imply that $\mathcal{L}$ is neither stable modulo 2 nor modulo 5. This strikingly contrasts with the known stability of the classical Fibonacci sequence modulo these both primes.

2000 Mathematics Subject Classification: 11B50, 11B39.
Keywords: Lucas sequence modulo prime powers, stability modulo primes.

Received November 30, 2009

1. Introduction and results

Niven [9] introduced the notion of uniform distribution of a sequence of integers as follows. Let $\mathcal{A} = (a_n)_{n=0,1,\ldots}$ be such a sequence and $m \geq 2$ an integer. $\mathcal{A}$ is called *uniformly distributed modulo* m (in the sequel mostly: u. d. mod m) if

$$\lim_{N\to\infty} \frac{1}{N} \cdot \#\{n < N : a_n \equiv b \pmod{m}\} = \frac{1}{m}$$

holds for any $b \in \{0, ..., m-1\}$. Sequences that are u. d. mod m are, e.g., of interest in the construction of numerical random number generators as for such a sequence the a_n/m are candidates for pseudo-random numbers uniformly distributed in $[0, 1[$. In this context it is specifically important to know under which conditions sequences defined by recurrences are u. d. mod m [4].

A decade after Niven's paper, Kuipers and Shiue [6] proved that the sequence $\mathcal{L} = (L_n)_{n=0,1,\ldots}$ of Lucas numbers, defined by

$$L_0 := 2,\ L_1 := 1,\ L_{n+2} := L_{n+1} + L_n \ \ (n \geq 0), \tag{1}$$

is not u. d. mod m for any integer $m \geq 2$. In the case of the Fibonacci sequence $\mathcal{F} = (F_n)_{n=0,1,\ldots}$, defined by

$$F_0 := 0,\ F_1 := 1,\ F_{n+2} := F_{n+1} + F_n \ \ (n \geq 0), \tag{2}$$

combination of work done by Kuipers and Shiue [7] and by Niederreiter [8] implied that $\mathcal{F}$ is u. d. mod m if and only if $m = 5^k,\ k \in \mathbb{N} := \{1, 2, ...\}$. An independent proof of this fact can be found in [1].

Almost at the same time when Niven's article [9] appeared, Wall [12] proved that second-order linear recurrences $\mathcal{A}$ 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 $m \in \mathbb{N}$. He explicitly determined the period length $h_{\mathcal{A}}(m)$ of $\mathcal{A}$ mod m in terms of a_0, a_1 and m. In particular, his Theorems 5 and 9 imply

$$h_{\mathcal{F}}(2^k) = h_{\mathcal{L}}(2^k) = 3 \cdot 2^{k-1}; \quad h_{\mathcal{F}}(5^k) = 4 \cdot 5^k,\ h_{\mathcal{L}}(5^k) = 4 \cdot 5^{k-1}$$

for any $k \in \mathbb{N}$. Clearly, if such a special linear recurring sequence $\mathcal{A}$ is u. d. modulo some $m \in \mathbb{N}$, then m divides $h_{\mathcal{A}}(m)$. Hence we see (what we already know from the above quotation) that the Fibonacci sequence is not u. d. mod 2^k whereas the Lucas sequence is neither u. d. mod 2^k nor mod 5^k. On the other hand, combination of Wall's formula $h_{\mathcal{F}}(5^k) = 4 \cdot 5^k$ with Niederreiter's result on the uniform distribution of $\mathcal{F}$ mod 5^k means that every $b \in \{0, ..., 5^k - 1\}$ appears exactly four times as residue mod 5^k in the period of $\mathcal{F}$ mod 5^k. But in the case of moduli m that are not pure powers of 5, the distribution of the residues mod m in a period of $\mathcal{F}$ mod m was relatively unexplored until the early 1990s.

At that time, Jacobson [3] explicitly described the function $v_{\mathcal{F}}(2^k, b), b \in \{0, ..., 2^k - 1\}$, for every $k \in \mathbb{N}$. Here

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

denotes the number of occurrences of the residue b mod m in the period of a recurring sequence $\mathcal{A}$ as above. Jacobson remarked in his introduction 'What makes this [complete description of $v_{\mathcal{F}}(2^k, .)$] possible is a type of stability that occurs when $k \geq 5$. This stability does not seem to appear for primes other than 2 and 5.' The precise definition of stability, not yet formally given in [3], depends on the set

$$\Omega_{\mathcal{A}}(m) := \{v_{\mathcal{A}}(m, b) \,|\, b \in \{0, ..., m-1\}\} \tag{3}$$

for all frequencies of residues mod m in a full period of $\mathcal{A}$ mod m. According to Carlip and Jacobson [2], 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 $k \geq k_0$. In these terms, we note $\Omega_{\mathcal{F}}(2^k) = \{0, 1, 2, 3, 8\}$ for every $k \geq 5$ as a consequence of Jacobson's main result in [3], whence the Fibonacci sequence $\mathcal{F}$ 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 u. d. mod m. Thus, one could say that the concept of stability was introduced to generalize uniform distribution modulo prime powers.

Since computation of the residue distribution of a stable sequence requires only a finite computational procedure, stability became an important tool in the study of frequency distribution. Thus, during the last decade, there appeared a series of papers on stability mod 2 of second-order linear recurrences $\mathcal{A}$ of the slightly more general type than above, namely $a_{n+2} = Aa_{n+1} + Ba_n$ $(n \geq 0)$ under various conditions on the integers A, B but in the uppermost number of cases with initial conditions $a_0 = 0, a_1 = 1$. Other articles examined stability modulo odd primes p. E.g., Somer and Carlip [11] exhibited several classes of second-order linear recurrences failing to be p-stable and provided sufficient criteria for such recurrences to be p-stable.

The aim of the present paper is to describe completely the function $v_{\mathcal{L}}(p^k, .)$ for $p = 2$ and $p = 5$. We begin with the case $p = 5$, which, according to general philosophy, should be the 'simpler' one, 5 being a divisor of (in fact, equal to) the discriminant of the companion polynomial $X^2 - X - 1$ of the recurrence in (1).

Theorem 1. *Suppose that $k \in \mathbb{N}$. Then, for every b from the least nonnegative residue system* $\bmod 5^k$*, one has*

$$(4)\quad v_{\mathcal{L}}(5^k, b) = \begin{cases} 5^{[(k-1)/2]}, & \text{if } b \equiv L_{5^{[k/2]}j} \pmod{5^k},\ j \in \{0,1,2,3\}, \\ 2 \cdot 5^{\ell}, & \text{if } b \equiv L_{2\cdot 5^{\ell}j + 5^{k-\ell-1}i},\ i \in \{0,1\},\ 0 \leq j < 5^{k-2\ell-1},\ 5 \nmid j \\ & \text{for some } \ell \in \{0, ..., [\frac{k}{2}] - 1\}, \\ 0 & \text{otherwise.} \end{cases}$$

Remark 1. Plainly, the second-mentioned case in (4) occurs only if $k \geq 2$. It is also evident that, in this case, exactly $8 \cdot 5^{k-2\ell-2}$ mod 5^k pairwise incongruent b's appear on the right-hand side of (4).

Remark 2. A simple calculation shows that, for given $k \in \mathbb{N}$, the third case in (4) holds for exactly $\frac{1}{3}(2 \cdot 5^k - 9 - 2 \cdot (-1)^k) > 0$ values of b. Hence asymptotically two third of the b's do not occur as a residue mod 5^k of any L_n.

By this last observation and definition (3), we immediately obtain

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

if $k \geq 2$, and $\Omega_{\mathcal{L}}(5) = \{0, 1\}$. This has the following consequence.

Corollary 1. *The Lucas sequence is not stable modulo* 5.

Next we come to the powers of 2.

Theorem 2. *Suppose $k \in \mathbb{N}, k \geq 3$. Then, for every b in the least nonnegative residue system* $\bmod 2^k$, *one has*

$$(5)\quad v_{\mathcal{L}}(2^k,b)=\begin{cases} 1, & \textit{if } b \equiv 1 \pmod 4, \\ 3, & \textit{if } b \equiv 3 \pmod 4, \\ 2, & \textit{if } b \equiv 4 \pmod 8, \\ 2^{[k/2]}, & \textit{if } b = 2, \\ 2^{[k/2]}, & \textit{if } b = 2^{2[(k-1)/2]}+2 \textit{ and } k \geq 5, \\ 16, & \textit{if } b \equiv 18 \pmod{128} \textit{ and } k \geq 7, \\ 2^\ell, & \textit{if } b \equiv 5\cdot 2^{2\ell-4}+2 \pmod{2^{2\ell-1}} \textit{for some}\, \ell \in \{5,...,[\frac{k+1}{2}]\}, \\ 0 & \textit{otherwise.} \end{cases}$$

Remark 3. We do not include here the values of $v_{\mathcal{L}}(2,b)$ and $v_{\mathcal{L}}(4,b)$ for $b=0,1$ and $b=0,1,2,3$, respectively. Clearly, the case covered by line 7 of formula (5) can occur only if $k \geq 9$.

Remark 4. Since the values of $\mathcal{L}$ mod 4 start with 2,1,3,0,3,3 and then repeat, one has the following equivalences

$$\begin{array}{lcl} L_n \equiv 1 \pmod 4 & \Leftrightarrow & n \equiv 1 \pmod 6, \\ L_n \equiv 3 \pmod 4 & \Leftrightarrow & n \equiv -1, \pm 2 \pmod 6, \\ L_n \equiv 4 \pmod 8 & \Leftrightarrow & n \equiv 3 \pmod 6, \\ L_n \equiv 2 \pmod{16} & \Leftrightarrow & n \equiv 0 \pmod 6, \end{array}$$

the third and fourth one being true by our Lemma 4, (ii) and (iii), respectively. Thus, the first three lines on the right-hand side of (5) refer exactly to the $n \not\equiv 0 \pmod 6$, whereas the lines 4 to 7 deal with the $n \in \{0,...,3\cdot 2^{k-1}-1\}$ divisible by 6. On the other hand, looking at the b's on the right-hand side of (5), we notice that in line 8 occur all b, which are congruent to 0 or 6 mod 8, all that are congruent to 10 mod 16, and exactly those congruent to 2 mod 16 not occurring in lines 4 through 7. Moreover, an easy calculation shows that, for any $k \geq 9$, the case in line 8 holds for exactly $\frac{1}{6}(143\cdot 2^{k-6}-15+(-1)^k) > 0$ values of b. Hence asymptotically about 37 % of the b's do not occur as residues mod 2^k of any L_n.

By this last statement and definition (3), we obtain

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

for any $k \geq 9$. Clearly, the sets $\Omega_{\mathcal{L}}(2^k)$ can be written down for $k=1,...,8$, too. This has the following consequence.

Corollary 2. *The Lucas sequence is not stable modulo* 2.

Of course, it would be interesting to determine, e.g., the function $v_{\mathcal{L}}(3^k, .)$ similarly to our Theorems 1 and 2. Our own experience with this problem is not just encouraging. In this context, the reader may compare the very partial results on $v_{\mathcal{F}}(3^k, .)$ in [10].

2. Some lemmas on Fibonacci and Lucas numbers

Let $\alpha := \frac{1}{2}(1+\sqrt{5}), \beta := \frac{1}{2}(1-\sqrt{5})$ denote the roots of the common companion polynomial $X^2 - X - 1$ of the Fibonacci and Lucas recurrence. Hence we have $\alpha^{n+2} = \alpha^{n+1} + \alpha^n$ for every $n \in \mathbb{Z}$ and the same equation with β instead of α. Defining, for each $n \in \mathbb{Z}$,

$$\Phi_n := \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad \Lambda_n := \alpha^n + \beta^n, \tag{6}$$

then the Φ's and Λ's satisfy the recurrences

$$\Phi_{n+2} = \Phi_{n+1} + \Phi_n, \quad \Lambda_{n+2} = \Lambda_{n+1} + \Lambda_n$$

and the initial conditions $\Phi_0 = 0,\ \Phi_1 = 1$ and $\Lambda_0 = 2,\ \Lambda_1 = 1$, respectively. Using (6) and $\alpha\beta = -1$ we easily find $\Phi_{-n} = (-1)^{n+1}\Phi_n, \Lambda_{-n} = (-1)^n\Lambda_n$ for any $n \in \mathbb{Z}$. Comparing this last fact with the definitions in (1) and (2), we obtain $\Phi_n = F_n, \Lambda_n = L_n$ for all $n \in \mathbb{N}_0 := \mathbb{N} \cup \{0\}$. Therefore, we may interpret the above Φ's and Λ's as 'continuation' of the F's and L's from $\mathbb{N}_0$ to $\mathbb{Z}$. This justifies to use the notations F_n and L_n, from now on, for the expressions on the right-hand sides in (6) for arbitrary $n \in \mathbb{Z}$.

Our first auxiliary result provides us with an expression for differences of Lucas numbers, and this will turn out to be a basic tool in our inquiry.

Lemma 1. *For all $s, t \in \mathbb{Z}$ of the same parity, the following alternative holds.*

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

Proof. With $q := (s+t)/2,\ r := (s-t)/2 \ \Leftrightarrow\ s = q+r,\ t = q-r$ we obtain, by (6) and $\alpha\beta = -1$,

$$\begin{aligned} L_{q+r} - L_{q-r} &= (\alpha^{q+r} - \alpha^{q-r}) + (\beta^{q+r} - \beta^{q-r}) = \alpha^q(\alpha^r - \varepsilon_r\beta^r) + \beta^q(\beta^r - \varepsilon_r\alpha^r) \\ &= (\alpha^q - \varepsilon_r\beta^q)(\alpha^r - \varepsilon_r\beta^r), \end{aligned}$$

whence our assertion. Note that we obviously put $\varepsilon_r := (-1)^r$. □

Lemma 2. *If $\ell \in \mathbb{N}_0$ and if $j, h \in \mathbb{Z}$ are incongruent* mod 4, *then*

$$L_{5^\ell j} \not\equiv L_{5^\ell h} \pmod{5}.$$

Proof. According to Lemma 1, the congruence $L_{5^\ell i} \equiv L_i \,(\mathrm{mod}\, 5)$ holds for any $i \in \mathbb{Z}$. On the other hand, we have $L_j \not\equiv L_h \,(\mathrm{mod}\, 5)$ since $\mathcal{L}$ has period 4 mod 5 and starts by 2,1,3,4, whence our assertion. □

The next two lemmas contain some divisibility properties of the Fibonacci and Lucas numbers. These properties will be of importance in our main proofs to precisely determine (or, in some cases, to estimate) the exact power of 5 or 2 occurring in the differences of certain Lucas numbers.

To formulate these statements conveniently, we first give the following definition (see Koblitz [5]). Let p be any prime number. For $z \in \mathbb{Z} \setminus \{0\}$, let $t \in \mathbb{N}_0$ be defined by the divisibility properties[1] $p^t \mid z$, $p^{t+1} \not| z$. Then we write $\mathrm{ord}_p z$ for this t and call it the p-adic ordinal of z, or shortly, 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 $z_1, z_2 \in \mathbb{Z}$. Note that it is often suitable to define additionally $\mathrm{ord}_p 0 := +\infty$ for any prime p. 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.

Our next lemma is basic for the proof of Theorem 1.

Lemma 3. *The equation* $\mathrm{ord}_5\, F_n = \mathrm{ord}_5\, n$ *holds for every $n \in \mathbb{Z}$.*

Proof. We may suppose $n \neq 0$. From Lemma 7 in [1] we immediately deduce $\mathrm{ord}_5\, F_n \leq \mathrm{ord}_5\, n$. To get the reversed inequality, we put $k := \mathrm{ord}_5\, n$, whence $n = 5^k j$ with some $j \in \mathbb{Z}, 5 \not| j$. From the first formula in (6) we infer the well-known divisibility property $F_{5^k} | F_n$, and thus $\mathrm{ord}_5\, F_{5^k} \leq \mathrm{ord}_5\, F_n$. Lemma 6 in [1] says $\mathrm{ord}_5\, F_{5^k} = k$ such that we are done. □

Our fourth and last lemma plays an important role in the proof of Theorem 2.

Lemma 4. *For $u, v \in \mathbb{Z}$, the following statements hold.*

(i) $3 \,|\, u \;\Leftrightarrow\; 2 \,|\, F_u \;\Leftrightarrow\; 2 \,|\, L_u$,

(ii) $3 \,|\, u, 6 \not| u \;\Rightarrow\; \mathrm{ord}_2\, F_u = 1,\ \mathrm{ord}_2\, L_u = 2$,

(iii) $6 \,|\, u \;\Rightarrow\; \mathrm{ord}_2\, F_u \geq 3,\ \mathrm{ord}_2\, L_u = 1,$ (*more precisely* : $\mathrm{ord}_2(L_u - 2) \geq 4$),

(iv) $2 \,|\, u \;\Rightarrow\; \mathrm{ord}_2\, F_{3u} = 2 + \mathrm{ord}_2\, u$.

Moreover, if $k \in \mathbb{N}, k \geq 3$, then one has

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

$$\textit{(v)}\qquad \operatorname{ord}_2(L_{3\cdot 2^{k-1}+u} - L_u) \begin{cases} = k & \textit{for } 3 \nmid u, \\ = k+1 & \textit{for } 3 \,|\, u, 6 \nmid u, \\ \geq k+3 & \textit{for } 6 \,|\, u. \end{cases}$$

Proof. (i): This is a consequence of the fact that both sequences $\mathcal{F}$ and $\mathcal{L}$ mod 2 begin with 0,1,1 and then repeat.
(ii): Since $\mathcal{F}$ mod 4 begins with 0,1,1,2,3,1 and then repeats, we have $F_u \equiv 2 \pmod 4$ for odd multiples u of 3. As already noticed in Remark 4, $\mathcal{L}$ mod 4 begins with 2,1,3,0,3,3 and then repeats, whence $\operatorname{ord}_2 L_u \geq 2$ for these same u's. In fact, we have here equality since no residue 0 occurs in $\mathcal{L}$ mod 8.
(iii): From (6) we see $F_v \,|\, F_u$ for every $v \neq 0$ dividing u. Hence $F_6 = 8$ divides F_u if $6 \,|\, u$. From the reasoning for (ii) we can also see $L_u \equiv 2 \pmod 4$ if $6 \,|\, u$. The sharpening of this fact will be proved at the end of (iv).
(iv): We may assume $u \neq 0$. Writing $u = 2^t v$ with odd $v \in \mathbb{Z}$ and iterating the formula $F_{2n} = F_n L_n$ (evident from (6)) sufficiently often, we obtain

$$F_{3u} = F_{3\cdot 2^t v} = F_{3v} \cdot \prod_{\tau=0}^{t-1} L_{3\cdot 2^\tau v}.$$

Using (ii) and (iii) this formula leads us to

$$\operatorname{ord}_2 F_{3u} = 1 + (t-1) + 2 = 2 + \operatorname{ord}_2 u.$$

as asserted. The sharpening of $\operatorname{ord}_2 L_u = 1$ for $6 \,|\, u$ can be established as follows. Note that $L_u - 2 = L_u - L_0$ equals $5F_{u/2}^2$ or $L_{u/2}^2$ according as $\frac{u}{2}$ is even or odd. In the first case, we find $\operatorname{ord}_2 (L_u - 2) = 2(2 + \operatorname{ord} \frac{u}{2}) \geq 6$ using (iv); in the second case we get $\operatorname{ord}_2 (L_u - 2) = 2 \operatorname{ord}_2 L_{u/2} = 4$, by (ii).
(v): Lemma 1 and (iv) lead to

$$\operatorname{ord}_2 (L_{3\cdot 2^{k-1}+u} - L_u) = \operatorname{ord}_2 (F_{3\cdot 2^{k-2}+u} F_{3\cdot 2^{k-2}}) = \operatorname{ord}_2 F_{3\cdot 2^{k-2}+u} + k.$$

If $3 \nmid u$, then $2 \nmid F_{3\cdot 2^{k-2}+u}$, by (i), and if $3 \,|\, u, 6 \nmid u$ then $2 \,\|\, F_{3\cdot 2^{k-2}+u}$ according to (ii). Finally, $6 \,|\, u$ leads to $\operatorname{ord}_2 F_{3\cdot 2^{k-2}+u} \geq 3$, by (iii). □

3. Proof of Theorem 1

The structure of this proof is as follows. First, we demonstrate two propositions relating to the first and second case in (4), respectively. Both propositions contain the phrase 'at least' twice. Having these results, our final argument implies, at a blow, 1) that all these 'at least' can be replaced by 'exactly' (hence showing the truth of formula (4) in the first two cases) and 2) that $v_{\mathcal{L}}(5^k, b) = 0$ for all b's not appearing in the first two cases.

Proposition 1. *Suppose that* $k \in \mathbb{N}$. *Then there are at least four distinct* $b \in \{0, ..., 5^k - 1\}$ *occurring at least* $5^{[(k-1)/2]}$ *times as residue* mod 5^k *of the* L_n *with* $0 \leq n < 4 \cdot 5^{k-1}$.

Proof. For $n, j \in \mathbb{Z}$ with $4 \,|\, n$ we deduce from Lemma 1

$$L_{n+5^{[k/2]}j} - L_{5^{[k/2]}j} = 5F_{(n/2)+5^{[k/2]}j}F_{n/2}$$

hence, by Lemma 3,

$$\text{ord}_5(L_{n+5^{[k/2]}j} - L_{5^{[k/2]}j}) = 1 + \text{ord}_5\Big(\frac{n}{2} + 5^{[k/2]}j\Big) + \text{ord}_5\frac{n}{2}. \tag{7}$$

Assuming, moreover, that

$$\text{ord}_5\frac{n}{2} \geq \Big[\frac{k}{2}\Big] \tag{8}$$

we obtain from (7)

$$\text{ord}_5(L_{n+5^{[k/2]}j} - L_{5^{[k/2]}j}) \geq 1 + 2\Big[\frac{k}{2}\Big] > 1 + 2\Big(\frac{k}{2} - 1\Big) = k - 1,$$

hence

$$L_{n+5^{[k/2]}j} \equiv L_{5^{[k/2]}j} \pmod{5^k}.$$

Condition (8) says that $5^{[k/2]}$ has to be a divisor of the even number $\frac{n}{2}$. Therefore, we write $n = 4 \cdot 5^{[k/2]} \cdot i$ with some $i \in \mathbb{N}_0, i < 5^{[(k-1)/2]}$. (Note here that $[\frac{k-1}{2}] + [\frac{k}{2}] = k-1$ for every $k \in \mathbb{Z}$.) Now, for every fixed $j \in \{0, 1, 2, 3\}$, we then have

$$0 \leq n + 5^{[k/2]}j = (4i + j)\, 5^{[k/2]} \leq (4 \cdot 5^{[(k-1)/2]} - 4 + 3)\, 5^{[k/2]} < 4 \cdot 5^{k-1}.$$

According to Lemma 2, the four numbers $L_{5^{[k/2]}j}$ $(j = 0, 1, 2, 3)$ are pairwise incongruent mod 5 hence, a fortiori, mod 5^k and Proposition 1 is proved. □

Proposition 2. *Suppose* $k \in \mathbb{N}, k \geq 2$. *Then, for every integer* ℓ *with* $0 \leq \ell \leq \frac{k}{2} - 1$, *there exist at least* $8 \cdot 5^{k-2\ell-2}$ *distinct* $b \in \{0, ..., 5^k - 1\}$ *occurring at least* $2 \cdot 5^{\ell}$ *times as residues* mod 5^k *of the* L_n *with* $0 \leq n < 4 \cdot 5^{k-1}$.

Proof. For all $n \in \mathbb{Z}$ with $\text{ord}_5 n = \ell$, we deduce from Lemmas 1 and 3

$$\text{ord}_5(L_{n+4\cdot5^{k-\ell-1}} - L_n) = \text{ord}_5(5F_{2\cdot5^{k-\ell-1}}F_{n+2\cdot5^{k-\ell-1}}) = 1 + (k - \ell - 1) + \ell = k,$$

where we essentially used the hypothesis $\ell \leq \frac{k}{2} - 1 \;\Leftrightarrow\; \ell < k - \ell - 1$. Hence we have $L_{n+4\cdot5^{k-\ell-1}} \equiv L_n \pmod{5^k}$ for all n as before. This means: If we want to count the integers n with $0 \leq n < 4 \cdot 5^{k-1}$ and $\text{ord}_5\, n = \ell$, for which a given b occurs as a residue of L_n mod 5^k, then we may determine the number of such n's satisfying $0 \le n < 4 \cdot 5^{k-\ell-1}$ and $\operatorname{ord}_5 n = \ell$, and multiply this number finally by 5^ℓ.

Therefore, we have to investigate the distribution of the $16 \cdot 5^{k-2\ell-2}$ numbers

$$(9) \qquad L_{5^\ell j} \quad (0 \le j < 4 \cdot 5^{k-2\ell-1},\ 5 \nmid j)$$

mod 5^k. We assert that half of them, i.e., $8 \cdot 5^{k-2\ell-2}$ of these L's, are pairwise incongruent mod 5^k, whereas the other half coincides mod 5^k with the first half. Of course, this implies Proposition 2.

We first show

$$L_{5^\ell(4 \cdot 5^{k-2\ell-1}-j)} \equiv L_{5^\ell j} \pmod{5^k}$$

for the *even* j as in (9). Indeed, we get from Lemmas 1 and 3

$$\operatorname{ord}_5(L_{5^\ell(4\cdot 5^{k-2\ell-1}-j)} - L_{5^\ell j}) = \operatorname{ord}_5(5F_{5^\ell(2\cdot 5^{k-2\ell-1}-j)}F_{2\cdot 5^{k-\ell-1}}) = 1+\ell+(k-\ell-1) = k.$$

Suppose now that j as in (9) is *odd*. We write either $j = 5^{k-2\ell-1}+i$ or $j = 3\cdot 5^{k-2\ell-1}+i$ with $|i| < 5^{k-2\ell-1}, 5 \nmid i$ but $2 \,|\, i$. We then have for both $\lambda \in \{1,3\}$

$$(10) \qquad \operatorname{ord}_5(L_{5^\ell(\lambda\cdot 5^{k-2\ell-1}+i)} - L_{5^\ell(\lambda\cdot 5^{k-2\ell-1}-i)}) = \operatorname{ord}_5(5F_{\lambda\cdot 5^{k-\ell-1}}F_{5^\ell i}) = k.$$

Having two j as in (9) but of distinct parity, then the corresponding $L_{5^\ell j}$ are incongruent mod 5, and thus mod 5^k. Hence we consider the $L_{5^\ell j}$ with $0 \le j < 2 \cdot 5^{k-2\ell-1}$, $5 \nmid j$, $2 \,|\, j$ and we assert that they are pairwise incongruent mod 5^k. Namely, let h, j satisfy $0 \le h < j < 2 \cdot 5^{k-2\ell-1}$, $5 \nmid hj$, $2 \,|\, h$, $2 \,|\, j$ and (w.l.o.g., compare Lemma 2) $4 \,|\, (j-h)$. Again according to Lemmas 1 and 3, we find

$$(11) \quad \operatorname{ord}_5(L_{5^\ell j} - L_{5^\ell h}) = \operatorname{ord}_5(5F_{5^\ell(j-h)/2}F_{5^\ell(j+h)/2}) = 1+2\ell+\operatorname{ord}_5\frac{j-h}{2}+\operatorname{ord}_5\frac{j+h}{2},$$

where the inequalities $0 < \frac{j-h}{2} < \frac{j+h}{2} < 2 \cdot 5^{k-2\ell-1}$ hold. By $5 \nmid hj$, at most one of the quotients $\frac{j-h}{2}, \frac{j+h}{2}$ is a multiple of 5. If this happens for none of these quotients, then (11) implies

$$\operatorname{ord}_5(L_{5^\ell j} - L_{5^\ell h}) = 1 + 2\ell \le k-1,$$

by our condition on ℓ in Proposition 2. Assume now $\omega := \operatorname{ord}_5\frac{j+h}{2} \in \mathbb{N}$ hence $\frac{j+h}{2} = \alpha \cdot 5^\omega$ with $\alpha \in \mathbb{N}$, $5 \nmid \alpha$. This implies $\alpha \cdot 5^\omega < 2 \cdot 5^{k-2\ell-1}$ and therefore $\omega \le k-2\ell-1$, where we are going to exclude equality. Namely, if $\omega = k-2\ell-1$, then $\alpha = 1$ hence $j+h = 2\cdot 5^{k-2\ell-1}$; from $j-h = 4\beta$ with some $\beta \in \mathbb{N}$ we would get $j = 5^{k-2\ell-1}+2\beta$, hence j would be odd. We thus obtain $\omega \le k-2\ell-2$, whence the estimate

$$(12) \qquad \operatorname{ord}_5(L_{5^\ell j} - L_{5^\ell h}) = 1 + 2\ell + 0 + \omega \le k-1,$$

from (11), and this means

$$(13) \qquad L_{5^\ell j} \not\equiv L_{5^\ell h} \pmod{5^k}.$$

If $\tilde{\omega} := \mathrm{ord}_5 \frac{j-h}{2} \in \mathbb{N}$, then $\omega = 0$ and from $0 < \frac{j-h}{2} < 5^{k-2\ell-1}$ we conclude $\tilde{\omega} \leq k - 2\ell - 2$ leading to (12) with ω replaced by $\tilde{\omega}$.

Next we have to consider odd j's as in (9). By virtue of the symmetry properties evident from (10), it is now enough to investigate the case $j = 3 \cdot 5^{k-2\ell-1} - i, h = 5^{k-2\ell-1} + g$ with $0 < g, i < 5^{k-2\ell-1}, 5 \not| \, gi$ and g, i both even. Since, again w.l.o.g., we may assume $4 \,|\, (j-h)$, we conclude from $j - h = 2 \cdot 5^{k-2\ell-1} - (g+i)$ that $\frac{g+i}{2}$ is odd leading immediately to $g \neq i$. Using once more Lemmas 1 and 3, we are led to

$$(14)\quad \mathrm{ord}_5(L_{5^\ell j} - L_{5^\ell h}) = 1 + 2\ell + \mathrm{ord}_5(5^{k-2\ell-1} - \frac{g+i}{2}) + \mathrm{ord}_5(2 \cdot 5^{k-2\ell-1} + \frac{g-i}{2}).$$

Here we distinguish the two cases according as the nonzero integer $\frac{g-i}{2}$ is or is not a multiple of 5. In the second case, the last summand on the right-hand side of (14) vanishes, whereas the next to the last is less than $k - 2\ell - 1$, whence (13). But if 5 divides $\frac{g-i}{2}$, then it cannot divide $\frac{g+i}{2}$, by $5 \not| \, gi$, and the third summand on the right-hand side of (14) vanishes. From $0 < |\frac{g-i}{2}| < 5^{k-2\ell-1}$ we obtain $\mathrm{ord}_5 \frac{g-i}{2} < k - 2\ell - 1$, hence again (13) from (14). □

Final Argument. The fact that in the three cases for b occurring in (4) the inequalities

$$(15)\qquad v_{\mathcal{L}}(5^k, b) \geq 5^{[(k-1)/2]}, \;\; v_{\mathcal{L}}(5^k, b) \geq 2 \cdot 5^\ell, \;\; \text{or} \;\; v_{\mathcal{L}}(5^k, b) \geq 0$$

hold, follows from Propositions 1, 2 or is a triviality, respectively. Thus, we obtain after a minor calculation using again $[\frac{k-1}{2}] + [\frac{k}{2}] = k - 1$

$$\sum_{b=0}^{5^k-1} v(5^k, b) \geq 4 \cdot 5^{[(k-1)/2]} + \sum_{\ell=0}^{[k/2]-1} (2 \cdot 5^\ell)(8 \cdot 5^{k-2\ell-2}) = 4 \cdot 5^{k-1}.$$

But the sum on the left-hand side trivially equals $h_{\mathcal{L}}(5^k)$, which is $4 \cdot 5^{k-1}$ according to Wall's formula quoted in our introduction. Therefore, we have equality in (15) for every residue b mod 5^k, no matter which one of the three cases applies, and this proves Theorem 1.

4. Proof of Theorem 2

Once and for all, *we suppose $k \geq 3$ in this whole section.* The structure of the proof is similar to that of Theorem 1 apart from one minor point. Namely, here we directly prove equalities for $v_{\mathcal{L}}(2^k, b)$ for all $b \not\equiv 2 \,(\mathrm{mod}\, 16)$ (see Propositions 3 and 4), whereas lower bounds for $v_{\mathcal{L}}(2^k, b)$ will appear, again as intermediate results, only for $b \equiv 2 \,(\mathrm{mod}\, 16)$ (see Propositions 5 through 8).

Our first result will cover just the case of odd b's in (5).

Proposition 3. *For every $d \in \{1, 2, 4, 5\}$, the numbers L_n with $n \in \{0, ..., 3 \cdot 2^{k-1} - 1\}$ and $n \equiv d \pmod 6$ are pairwise incongruent* mod 2^k.

Applying this to $d = 1$ and $d \in \{2, 4, 5\}$, respectively, and taking the first two equivalences of Remark 4 into account, we deduce $v_{\mathcal{L}}(2^k, b) = 1$ for $b \equiv 1 \pmod 4$ and $v_{\mathcal{L}}(2^k, b) = 3$ for $b \equiv 1 \pmod 4$. These are just the first two lines of formula (5).

Proof. We have to show that the L_{6j+d} with $0 \leq j < 2^{k-2}$ are pairwise incongruent mod 2^k. To this purpose, let $0 \leq i < j < 2^{k-2}$ and consider[2]

$$L_{6j+d} - L_{6i+d} = \begin{cases} 5F_{3(j+i)+d}F_{3(j-i)} & \text{if } j - i \text{ is even,} \\ L_{3(j+i)+d}L_{3(j-i)} & \text{if } j - i \text{ is odd,} \end{cases} \tag{16}$$

according to Lemma 1. By Lemma 4 (i), both of $F_{3(j+i)+d}, L_{3(j+i)+d}$ are odd. If $j - i$ is even, then the first alternative in (16) leads to

$$\operatorname{ord}_2(L_{6j+d} - L_{6i+d}) = \operatorname{ord}_2 F_{3(j-i)} = 2 + \operatorname{ord}_2(j - i),$$

where we used Lemma 4 (ii). Since $0 < j - i < 2^{k-2}$ we have $\operatorname{ord}_2(j - i) \leq k - 3$ hence

$$L_{6j+d} \not\equiv L_{6i+d} \pmod{2^k}. \tag{17}$$

If $j - i$ is odd, then the second alternative in (16) and Lemma 4 (ii) together imply

$$\operatorname{ord}_2(L_{6j+d} - L_{6i+d}) = \operatorname{ord}_2 L_{3(j-i)} = 2,$$

which is less than k, whence again (17). □

Our next result will cover just the case $b \equiv 4 \pmod 8$ in (5).

Proposition 4. *All $b \in \{0, ..., 2^k - 1\}$ with $b \equiv 4 \pmod 8$ occur exactly once as residue* mod 2^k *of some L_n with $0 \leq n < 3 \cdot 2^{k-2}$ and $n \equiv 3 \pmod 6$. Moreover, for these n, the following congruence holds*

$$L_{3 \cdot 2^{k-2} + n} \equiv L_n \pmod{2^k}. \tag{18}$$

With the third equivalence of Remark 4 in mind, Proposition 4 says nothing but $v_{\mathcal{L}}(2^k, b) = 2$ for $b \equiv 4 \pmod 8$.

[2] We note here for later purposes that (16) holds for any $d \in \mathbb{Z}$.

Proof. We have exactly 2^{k-3} residues b as specified and the same number of n's mentioned in the first sentence. Since $L_3 = 4, L_9 = 76$ show the truth of the proposition for $k = 3$, we may assume $k \geq 4$. To see the truth of the first assertion, we shall apply (16) with $d = 3$ and $0 \leq i < j < 2^{k-3}$. If $j - i$ is even, then $3(j + i + 1) \equiv 3 \pmod 6$, hence $\operatorname{ord}_2 F_{3(j+i+1)} = 1$ by Lemma 4 (ii), and the first alternative in (16) leads to

$$\operatorname{ord}_2 (L_{6j+3} - L_{6i+3}) = 1 + \operatorname{ord}_2 F_{3(j-i)} = 3 + \operatorname{ord}_2 (j - i)$$

using also Lemma 4 (iv). Since $\operatorname{ord}_2 (j - i) \leq k - 4$ we get (17) with $d = 3$. In the case of odd $j - i$, the number $3(j + i + 1)$ is a multiple of 6, whence $\operatorname{ord}_2 L_{3(j+i+1)} = 1$, by Lemma 4 (iii). The second alternative in (16) combined with $3(j - i) \equiv 3 \pmod 6$ then leads to

$$\operatorname{ord}_2(L_{6j+3} - L_{6i+3}) = 1 + \operatorname{ord}_2 L_{3(j-i)} = 3,$$

by Lemma 4 (ii). Since we assumed $k > 3$, (17) holds also in this case.

To prove (18) for the n's as specified there, we note

$$L_{6(2^{k-3}+j)+3} - L_{6j+3} = 5F_{3(2j+2^{k-3}+1)}F_{3\cdot 2^{k-3}}$$

since $3 \cdot 2^{k-3}$ is even, by $k \geq 4$. In virtue of $3(2j + 2^{k-3} + 1) \equiv 3 \pmod 6$ and Lemma 4 (ii),(iv), we infer from the last equation

$$\operatorname{ord}_2(L_{6(2^{k-3}+j)+3} - L_{6j+3}) = 1 + (k - 1) = k,$$

whence (18). □

The following Propositions 5 through 8 all concern the remaining case $b \equiv 2$ (mod 16).

Proposition 5. *For all $n = 3 \cdot 2^{[(k-1)/2]}j$ with $0 \leq j < 2^{[k/2]}$, the congruence*

$$L_n \equiv 2 \pmod{2^k} \tag{19}$$

holds. This implies $v_{\mathcal{L}}(2^k, 2) \geq 2^{[k/2]}$.

Proof. For $k = 3$ and $k = 4$, one can directly check the L_{6j} with $0 \leq j < 2$ and $0 \leq j < 4$ mod 8 and mod 16, respectively. Assuming now $k \geq 5$, we have $\ell := [\frac{k-1}{2}] \geq 2$, and hence, by Lemma 1,

$$L_n - 2 = L_{3\cdot 2^\ell j} - L_0 = 5F^2_{3\cdot 2^{\ell-1}j}$$

since $3 \cdot 2^{\ell-1}j$ is even. Then Lemma 4 (iv) leads to

$$\operatorname{ord}_2(L_n - 2) = 2 \operatorname{ord}_2 F_{3\cdot 2^{\ell-1}j} \geq 2(\ell + 1) > k - 1,$$

whence (19). □

Proposition 6. *Suppose $k \geq 5$ and define $\ell := [\frac{k-1}{2}]$. Then the congruences* mod 2^k

$$(20) \qquad L_{3\cdot 2^{\ell-1}} \equiv 2^{2\ell} + 2, \quad L_{3\cdot 2^{\ell-1}(2j+1)} \equiv L_{3\cdot 2^{\ell-1}} \quad (j \in \mathbb{Z})$$

hold implying $v_{\mathcal{L}}(2^k, 2^{2[(k-1)/2]} + 2) \geq 2^{[k/2]}$.

Proof. If $\ell \geq 3 \;\Leftrightarrow\; k \geq 7$, then we have with some odd integer u

$$L_{3\cdot 2^{\ell-1}} - L_0 = 5F^2_{3\cdot 2^{\ell-2}} = (1+4)\cdot(2^\ell u)^2 \equiv 2^{2\ell} \pmod{2^{2\ell+2}},$$

by Lemma 4 (iv). Since $2(\ell+1) \geq k$ we have the first congruence in (20). Note that $L_6 = 18$ gives its truth also for $k = 5$ and $k = 6$. If $k \geq 5 \Leftrightarrow \ell \geq 2$, then the second congruence in (20) is obtained from

$$\mathrm{ord}_2(L_{3\cdot 2^{\ell-1}(2j+1)} - L_{3\cdot 2^{\ell-1}}) \geq 2(\ell+1)+1 > k$$

for all $j \in \mathbb{Z}$.

To get the final implication, note that, for the integers j with $0 \leq j < 2^{k-\ell-1}$, the number $3\cdot 2^{\ell-1}(2j+1)$ belongs to $\{0, ..., 3\cdot 2^{k-1}-1\}$. □

Proposition 7. *For $k \geq 7$ one has the following assertions.*
a) The numbers L_{12j+6} with $0 \leq j < 2^{k-7}$ are pairwise incongruent mod 2^k*; these are, in some order, congruent to the distinct $b \in \{0, ..., 2^k - 1\}$ with $b \equiv 18 \pmod{128}$.*
b) $L_{12(2^{k-6}-j)-6} \equiv L_{12j+6} \pmod{2^k}$ for all $j \in \mathbb{Z}$.
c) $L_{3\cdot 2^{k-4}+n} \equiv L_n \pmod{2^k}$ for all multiples n of 6.
Together these statements imply $v_{\mathcal{L}}(2^k, b) \geq 16$ for any $b \equiv 18 \pmod{128}$.

Proof. a) Here we may suppose $k \geq 8$. With $0 \leq i < j < 2^{k-7}$ we consider the equation

$$(21) \qquad L_{12j+6} - L_{12i+6} = 5F_{6(j+i+1)}F_{6(j-i)}.$$

Exactly one of the numbers $j+i+1$ bzw $j-i$ is odd, and the 2-order of the corresponding F equals to 3. On the other hand, we find $0 < j-i < j+i+1 < 2^{k-6}$. Hence the 2-order of the $F_{6(...)}$ with the even (...) is less than or equal to $k-4$. Thus, (21) leads to our first claim. As to the second one, we apply (21) with $i = 0$ to find

$$\mathrm{ord}_2(L_{12j+6} - 18) = \mathrm{ord}_2 F_{6(j+1)} + \mathrm{ord}_2 F_{6j} = 4 + \mathrm{ord}_2 2(j+1) + \mathrm{ord}_2 2j \geq 7$$

since j or $j+1$ is even. Therefore, we obtain $L_{12j+6} \equiv 18$ modulo $2^7 = 128$.
b) By $L_{-n} = L_n$ for even n, it is enough to consider the difference

$$L_{3\cdot 2^{k-4}-(12j+6)} - L_{-(12j+6)}.$$

According to the third case of Lemma 4 (v) its 2-order is at least k.
c) Again by Lemma 4 (v), the difference $L_{3\cdot 2^{k-4}+n} - L_n$ has 2-order at least k since n is divisible by 6.

To obtain the final conclusion, notice that, among the L_{12j+6} with $0 \le j < 2^{k-6}$, each b as in a) occurs exactly twice as residue mod 2^k, by b). Using c) we next deduce from this last fact that, for every $t \in \{1, ..., 8\}$, there are exactly two $j \in \{(t-1)\cdot 2^{k-6}, ..., t\cdot 2^{k-6} - 1\}$ such that the corresponding L_{12j+6} are congruent mod 2^k to a given b as in a). (Note $12 \cdot (8 \cdot 2^{k-6} - 1) + 6 = 3 \cdot 2^{k-1} - 6$ is the last odd multiple of 6 less than $3 \cdot 2^{k-1}$.) □

Proposition 8. *If $k \ge 9$, then, for every $\ell \in \{5, ..., [\frac{k+1}{2}]\}$, the following statements hold.*
a) For any $j \in \mathbb{Z}$, one has

$$L_{3\cdot 2^{\ell-3}(2j+1)} \equiv 5 \cdot 2^{2\ell-4} + 2 \pmod{2^{2\ell-1}}. \tag{22}$$

b) The numbers $L_{3\cdot 2^{\ell-3}(2j+1)}$ with $0 \le j < 2^{k-2\ell+1}$ are pairwise incongruent $\bmod 2^k$.
c) For all $j \in \mathbb{Z}$, one has the congruence

$$L_{3\cdot 2^{\ell-3}(2^{k-2\ell+3}-2j-1)} \equiv L_{3\cdot 2^{\ell-3}(2j+1)} \pmod{2^k}.$$

d) For all $j \in \mathbb{Z}$, one has

$$L_{3\cdot 2^{k-\ell}+3\cdot 2^{\ell-3}(2j+1)} \equiv L_{3\cdot 2^{\ell-3}(2j+1)} \pmod{2^k}.$$

All these claims together imply $v_{\mathcal{L}}(2^k, 5 \cdot 2^{2\ell-4} + 2) \ge 2^\ell$.

Proof. a) Notice first that, using Lemma 4 (iv), we have with some odd u

$$L_{3\cdot 2^{\ell-3}} - L_0 = 5F^2_{3\cdot 2^{\ell-4}} = 5 \cdot (2^{\ell-2}u)^2 \equiv 5 \cdot 2^{2\ell-4} \pmod{2^{2\ell-1}},$$

which is (22) for $j = 0$. Furthermore, we find from

$$L_{3\cdot 2^{\ell-3}(2j+1)} - L_{3\cdot 2^{\ell-3}} = 5F_{3\cdot 2^{\ell-3}(j+1)}F_{3\cdot 2^{\ell-3}j}$$

that the 2-order of this difference is at least $2\ell - 1$, whence (22) for any j.
b) If k is odd and $\ell = (k+1)/2$, then there is nothing to be proved. But if $\{0, ..., 2^{k-2\ell+1} - 1\}$ contains two distinct numbers, say, $0 \le i < j < 2^{k-2\ell+1}$, then we consider

$$L_{3\cdot 2^{\ell-3}(2j+1)} - L_{3\cdot 2^{\ell-3}(2i+1)} = 5F_{3\cdot 2^{\ell-3}(j+i+1)}F_{3\cdot 2^{\ell-3}(j-i)}.$$

The 2-order of this difference is at most $2(\ell-1) + (k - 2\ell + 1) = k - 1$ since $0 < j - i < j + i + 1 < 2^{k-2\ell+2}$ and exactly one of the numbers $j + i + 1, j - i$ is odd.
c) From

$$L_{3\cdot 2^{k-\ell}-3\cdot 2^{\ell-3}(2j+1)} - L_{3\cdot 2^{\ell-3}(2j+1)} = 5F_{3\cdot 2^{k-\ell-1}}F_{3\cdot 2^{k-\ell-1}-3\cdot 2^{\ell-3}(2j+1)}$$

we see that the 2-order of the difference is at least $(k-\ell+1)+(\ell-1)=k$.
d) Starting from

$$L_{3\cdot 2^{k-\ell}+3\cdot 2^{\ell-3}(2j+1)} - L_{3\cdot 2^{\ell-3}(2j+1)} = 5F_{3\cdot 2^{k-\ell-1}}F_{3\cdot 2^{k-\ell-1}+3\cdot 2^{\ell-3}(2j+1)}$$

we conclude as in c).

The subscript $3\cdot 2^{\ell-3}(2j+1)$ of the Lucas number in (22) belongs to $\{0,...,3\cdot 2^{k-1}-1\}$ if and only if $0\le j<2^{k-\ell+1}$. According to a) and b) there is exactly one $j_0\in\{0,...,2^{k-2\ell+1}-1\}$, for which the corresponding $L_{3\cdot 2^{\ell-3}(2j_0+1)}$ is congruent to $5\cdot 2^{2\ell-4}+2 \bmod 2^k$. The above set $\{0,...,2^{k-\ell+1}-1\}$ decomposes into 2^ℓ disjoint subsets of successive integers of the form $S_\lambda:=\{\lambda\cdot 2^{k-2\ell+1},...,(\lambda+1)\cdot 2^{k-2\ell+1}-1\}$ with $\lambda=0,...,2^\ell-1$. Then c) and d) imply that, in each of these S_λ, there is exactly one j_λ such that $L_{3\cdot 2^{\ell-3}(2j_\lambda+1)}$ is congruent to $5\cdot 2^{2\ell-4}+2 \bmod 2^k$, whence the lower bound for $v_{\mathcal{L}}(2^k,5\cdot 2^{2\ell-4}+2)$. Notice that our information on the j_λ is much more precise (than only $j_\lambda\in S_\lambda$) as far as the exact position of j_λ in S_λ is explicitely determined by the position of j_0 in S_0. □

Final Argument. According to our statement directly after Proposition 3 and at the end of Proposition 4, we have

$$\sum_{\substack{0\le b<2^k\\ b\not\equiv 2\,(16)}} v_{\mathcal{L}}(2^k,b)=1\cdot 2^{k-2}+3\cdot 2^{k-2}+2\cdot 2^{k-3}=5\cdot 2^{k-2}.$$

Using this and Wall's formula $h_{\mathcal{L}}(2^k)=3\cdot 2^{k-1}$, we obtain

$$\sum_{\substack{0\le b<2^k\\ b\equiv 2\,(16)}} v_{\mathcal{L}}(2^k,b)=2^{k-2}. \tag{23}$$

Now, for $k=3$ and $k=4$, the equality $2^{k-2}=2^{[k/2]}$ holds, whence, by (23) and Proposition 5, $v_{\mathcal{L}}(2^k,2)=2^{[k/2]}$ and $v_{\mathcal{L}}(2^k,b)=0$ for all $b\equiv 2\,(\mathrm{mod}\,16), b\ne 2$. Next, for $k=5$ and $k=6$, we have $2^{[k/2]}+2^{[k/2]}=2^{k-2}$; therefore (23) and Propositions 5 and 6 imply $v_{\mathcal{L}}(2^k,b)=2^{[k/2]}$ for $b\in\{2,2^{2[(k-1)/2]}+2\}$, and $v_{\mathcal{L}}(2^k,b)=0$ for all other $b\equiv 2\,(\mathrm{mod}\,16)$. If $k\ge 7$, then the b's in the sixth line on the right-hand side of (5) are just the $128j+18$ with $0\le j<2^{k-7}$. For $k=7$ and $k=8$, one sees $2\cdot 2^{[k/2]}+16\cdot 2^{k-7}=2^{k-2}$; plainly, we use here (23) and Propositions 5, 6 and 7 to conclude. Suppose finally $k\ge 9$. Note that the b's in the seventh line in (5) can be written, for every $\ell\in\{5,...,[(k+1)/2]\}$, in the form

$$2^{2\ell-1}j+5\cdot 2^{2\ell-4}+2\ \ (0\le j<2^{k-2\ell+1}).$$

Then, by Proposition 8, the contribution of line 7 to the left-hand side of (23) is at least

$$\sum_{\ell=5}^{[(k+1)/2]} 2^\ell\cdot 2^{k-2\ell+1}=2^{k-3}-2^{[k/2]+1}.$$

Thus, for $k \geq 9$, the contribution of the b's specified in lines 4 through 7 of (5) to the left-hand side of (23) is at least

$$2 \cdot 2^{[k/2]} + 16 \cdot 2^{k-7} + (2^{k-3} - 2 \cdot 2^{[k/2]}) = 2^{k-2}.$$

This means that all lower bounds for the $v_{\mathcal{L}}(2^k, b)$ appearing at the end of Propositions 5 through 8, in fact, are equalities and, moreover, that $v_{\mathcal{L}}(2^k, b) = 0$ holds for all residues b mod 2^k not mentioned in lines 4 through 7 of formula (5).

REFERENCES

[1] BUNDSCHUH, P.: *On the distribution of Fibonacci numbers*, Tamkang J. Math. **5** (1974), 75-79.

[2] CARLIP, W.; JACOBSON, E. T.: *Unbounded stability of two-term recurrence sequences modulo* 2^k, Acta Arith. **74** (1996), 329-346.

[3] JACOBSON, E. T.: *Distribution of the Fibonacci numbers mod* 2^k, Fibonacci Quart. **30** (1992), 211-215.

[4] KNUTH, D.E.: *Seminumerical Algorithms. The Art of Computer Programming*, Vol. 2, 2nd ed., Addison Wesley, Reading, MA, 1981.

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

[6] KUIPERS, L.; SHIUE, J.-S.: *A distribution property of the sequence of Lucas numbers*, Elem. Math. **27** (1972), 10-11.

[7] KUIPERS, L.; SHIUE, J.-S.: *A distribution property of the sequence of Fibonacci numbers*, Fibonacci Quart. **10** (1972), 375-377.

[8] NIEDERREITER, H.: *Distribution of Fibonacci numbers* mod 5^k, Fibonacci Quart. **10** (1972), 373-374.

[9] NIVEN, I.: *Uniform distribution of sequences of integers*, Trans. Amer. Math. Soc. **98** (1961), 52-61.

[10] SHIU, W. C.; CHU, C. I.: *Distribution of the Fibonacci numbers modulo* 3^k, Fibonacci Quart. **43** (2005), 22-28.

[11] SOMER, L.; CARLIP, W.: *Stability of second-order recurrences modulo* p^r, Int. J. Math. Math. Sci. **23** (2000), 225-241.

[12] WALL, D. D.: *Fibonacci series modulo m*, Amer. Math. Monthly **67** (1960), 525-532.

Peter Bundschuh
Universität zu Köln
Mathematisches Institut
Weyertal 86-90
50931 Köln
Germany
e-mail: pb@math.uni-koeln.de

Ralf Bundschuh
The Ohio State University
Department of Physics
191 West Woodruff Ave
Columbus, OH 43210
U.S.A.
e-mail: bundschuh@mps.ohio-state.edu