POLITECNICO DI TORINO
Repository ISTITUZIONALE

On the l.c.m. of shifted Lucas numbers

Original
On the l.c.m. of shifted Lucas numbers / Sanna, Carlo. - In: INDAGATIONES MATHEMATICAE. - ISSN 0019-3577. - STAMPA. - (2022). [10.1016/j.indag.2022.04.006]

Availability:
This version is available at: 11583/2962874 since: 2022-05-06T17:46:15Z

Publisher:
Elsevier

Published
DOI:10.1016/j.indag.2022.04.006

Terms of use:

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright

(Article begins on next page)

24 April 2024

arXiv:2108.03628v1 [math.NT] 8 Aug 2021

ON THE L.C.M. OF SHIFTED LUCAS NUMBERS

CARLO SANNA†

Abstract. Let $(L_n)_{n \geq 1}$ be the sequence of Lucas numbers, defined recursively by $L_1 := 1$, $L_2 := 3$, and $L_{n+2} := L_{n+1} + L_n$, for every integer $n \geq 1$. We determine the asymptotic behavior of $\log \operatorname{lcm}(L_1 + s_1, L_2 + s_2, \dots, L_n + s_n)$ as $n \to +\infty$, for $(s_n)_{n \geq 1}$ a periodic sequence in $\{-1, +1\}$. We also carry out the same analysis for $(s_n)_{n \geq 1}$ a sequence of independent and uniformly distributed random variables in $\{-1, +1\}$. These results are Lucas numbers-analogs of previous results obtained by the author for the sequence of Fibonacci numbers.

1. Introduction

Let $(F_n)_{n \geq 1}$ be the sequence of Fibonacci numbers, defined recursively by $F_1 := 1$, $F_2 := 1$, and $F_{n+2} := F_{n+1} + F_n$ for every integer $n \geq 1$. Guy and Matiyasevich [10] proved that

$$\log \operatorname{lcm}(F_1, F_2, \dots, F_n) \sim \frac{3 \log \alpha}{\pi^2} \cdot n^2 \qquad (n \to +\infty), \tag{1}$$

where lcm denotes the least common multiple and $\alpha := \big(1 + \sqrt{5}\big)/2$ is the golden ratio. This result was generalized to Lucas sequences, Lehmer sequences, and other sequences with special divisibility properties [1–4, 6, 8, 9, 17].

Motivated by (1), the author considered the least common multiple of *shifted* Fibonacci numbers $F_k \pm 1$, and proved two results [13]. The first regards periodic sequences of signs:

Theorem 1.1. *For every periodic sequence $\mathbf{s} = (s_n)_{n \geq 1}$ in $\{-1, +1\}$, there exists an effectively computable rational number $A_{\mathbf{s}} > 0$ such that*

$$\log \operatorname{lcm}(F_1 + s_1, F_2 + s_2, \dots, F_n + s_n) \sim A_{\mathbf{s}} \cdot \frac{\log \alpha}{\pi^2} \cdot n^2 \qquad (n \to +\infty).$$

(Zero terms in the least common multiple are ignored.)

By "effectively computable" we mean that there exists an algorithm that, given as input the period of the periodic sequence $\mathbf{s}$, returns as output the numerator and denominator of the rational number $A_{\mathbf{s}}$. Indeed, the author computed $A_{\mathbf{s}}$ for periodic sequences with period length not exceeding 6 [13, Tables 1, 2].

The second result regards random sequences of signs. (For similar results on the least common multiple of random sequences, see [5, 7, 12, 14, 15].)

Theorem 1.2. *Let $(s_n)_{n \geq 1}$ be a sequence of independent random variables that are uniformly distributed in $\{-1, +1\}$. Then*

$$\mathbb{E}\big[\log \operatorname{lcm}(F_1 + s_1, F_2 + s_1, \dots, F_n + s_n)\big] \sim \frac{45 \operatorname{Li}_2\big(\frac{1}{16}\big)}{2} \cdot \frac{\log \alpha}{\pi^2} \cdot n^2 \qquad (n \to +\infty),$$

where $\operatorname{Li}_2(z) := \sum_{n=1}^{\infty} z^n / n^2$ denotes the dilogarithm.

The purpose of this paper is to establish the analogs of Theorems 1.1 and 1.2 for the sequence of Lucas numbers $(L_n)_{n \geq 1}$, defined recursively by $L_1 := 1$, $L_2 := 3$, and $L_{n+2} := L_{n+1} + L_n$ for every integer $n \geq 1$. We remark that the analog of (1) is

$$\log \operatorname{lcm}(L_1, L_2, \dots, L_n) \sim \frac{4 \log \alpha}{\pi^2} \cdot n^2 \qquad (n \to +\infty),$$

2010 *Mathematics Subject Classification.* Primary: 11B39, Secondary: 11B37, 11N37.

Key words and phrases. asymptotic formula; least common multiple; Lucas number.

† C. Sanna is a member of GNSAGA of INdAM and of CrypTO, the group of Cryptography and Number Theory of Politecnico di Torino.

which follows from a result of Bézivin [6].

Our first result is the following analog of Theorem 1.1.

Theorem 1.3. *For every periodic sequence* $\mathbf{s} = (s_n)_{n\geq 1}$ *in* $\{-1, +1\}$*, there exists an effectively computable rational number* $B_{\mathbf{s}} > 0$ *such that*

$$\log \operatorname{lcm}(L_1 + s_1, L_2 + s_2, \ldots, L_n + s_n) \sim B_{\mathbf{s}} \cdot \frac{\log \alpha}{\pi^2} \cdot n^2 \qquad (n \to +\infty).$$

We computed $B_{\mathbf{s}}$ for periodic sequences with period length at most 6, see Table 1. We notice that for such sequences $A_{\mathbf{s}}$ takes 8 different values, while $B_{\mathbf{s}}$ takes 58.

Table 1. Values of $B_{\mathbf{s}}$ for periodic sequences $\mathbf{s}$ with period length at most 6.

$\mathbf{s}$	$D_{\mathbf{s}}$	$\mathbf{s}$	$D_{\mathbf{s}}$	$\mathbf{s}$	$D_{\mathbf{s}}$	$\mathbf{s}$	$D_{\mathbf{s}}$
−	7/2	−−++−	128399/46080	−−−−++	601/192	+−−−+−	581/192
+	45/16	−−+++	24931/9216	−−−+−−	103/32	+−−−++	179/64
−+	45/16	−+−−−	1801/576	−−−+−+	287/96	+−−+−+	65/24
+−	7/2	−+−−+	3095/1024	−−−++−	73/24	+−−++−	527/192
−−+	179/64	−+−+−	1163/384	−−−+++	45/16	+−−+++	161/64
−+−	73/24	−+−++	8917/3072	−−+−−−	581/192	+−+−−−	99/32
−++	45/16	−++−−	62909/23040	−−+−+−	215/64	+−+−−+	93/32
+−−	139/48	−++−+	2195/768	−−+−++	601/192	+−+−++	157/48
+−+	65/24	−+++−	12331/4608	−−++−−	527/192	+−++−−	139/48
++−	493/192	−++++	133/48	−−++−+	161/64	+−+++−	103/32
−−−+	45/16	+−−−−	2399/768	−−+++−	73/24	+−++++	287/96
−−+−	91/32	+−−−+	4339/1536	−−++++	45/16	++−−−−	139/48
−−++	9/4	+−−+−	4531/1536	−+−−−−	103/32	++−−−+	65/24
−+−−	7/2	+−−++	60269/23040	−+−−−+	287/96	++−−+−	527/192
−++−	47/16	+−+−−	763/256	−+−−++	45/16	++−−++	161/64
−+++	9/4	+−+−+	739/256	−+−+−−	73/24	++−+−−	87/32
+−−−	25/8	+−++−	409/144	−+−++−	557/192	++−+−+	81/32
+−−+	39/16	+−+++	1055/384	−+−+++	171/64	++−+++	449/192
+−++	45/16	++−−−	1603/576	−++−−−	527/192	+++−−−	139/48
++−−	3	++−−+	1549/576	−++−−+	161/64	+++−−+	65/24
++−+	39/16	++−+−	4361/1536	−++−+−	73/24	+++−+−	103/32
+++−	7/2	++−++	12455/4608	−+++−−	493/192	+++−++	287/96
−−−−+	4087/1280	+++−−	4043/1536	−+++−+	449/192	++++−−	87/32
−−−+−	9709/3072	+++−+	2107/768	−++++−	557/192	++++−+	81/32
−−−++	130987/46080	++++−	2113/768	−+++++	171/64	+++++−	73/24
−−+−−	5981/1920	−−−−−+	157/48	+−−−−−	99/32		
−−+−+	1735/576	−−−−+−	215/64	+−−−−+	93/32		

Our second result is the following analog of Theorem 1.2.

Theorem 1.4. *Let* $(s_n)_{n\geq 1}$ *be a sequence of independent random variables that are uniformly distributed in* $\{-1, +1\}$*. Then*

$$\mathbb{E}\big[\log \operatorname{lcm}(L_1 + s_1, L_2 + s_1, \ldots, L_n + s_n)\big] \sim C \cdot \frac{\log \alpha}{\pi^2} \cdot n^2 \qquad (n \to +\infty),$$

where

$$C := \tfrac{243}{128} + \tfrac{27}{8}\operatorname{Li}_2\!\big(\tfrac{1}{4}\big) + \tfrac{9}{8}\operatorname{Li}_2\!\big(\tfrac{1}{16}\big) + \tfrac{3}{16}\operatorname{Li}_2\!\big(\tfrac{1}{16}; \tfrac{1}{3}\big) + \tfrac{3}{32}\operatorname{Li}_2\!\big(\tfrac{1}{16}; \tfrac{2}{3}\big)$$

and $\operatorname{Li}_2(z; a) := \sum_{n=1}^{\infty} z^n/(n+a)^2$.

The proofs of Theorems 1.3 and 1.4 employ methods similar to those used in the proofs of Theorems 1.1 and 1.2. However, the details are more involved because the multiplicative expressions of shifted Lucas numbers in terms of Fibonacci and Lucas numbers (see Lemma 3.6 below) are more complex than those of shifted Fibonacci numbers (see [13, Lemma 2.3]).

2. Notation

We employ the Landau–Bachmann "Big Oh" notation O with its usual meaning. Any dependence of the implied constants is indicated with subscripts. We let $\lfloor x \rfloor$ denote the greatest integer not exceeding x. We reserve the letter p for prime numbers, and we write $\nu_p(n)$, $\varphi(n)$, and $\mu(n)$, for the p-adic valuation, the Euler function, and the Möbius function of a positive integer n, respectively.

3. Preliminaries on Fibonacci and Lucas numbers

It is well known that the Binet formulas

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad L_n = \alpha^n + \beta^n, \tag{2}$$

where $\alpha := \big(1 + \sqrt{5}\big)/2$ and $\beta := \big(1 - \sqrt{5}\big)/2$, hold for every integer $n \geq 1$. Let $\Phi_1 := 1$ and

$$\Phi_n := \prod_{\substack{1 \leq k \leq n \\ (n,k)=1}} \left(\alpha - \mathrm{e}^{\frac{2\pi \mathrm{i} k}{n}} \beta\right) \tag{3}$$

for every integer $n \geq 2$. It can be proved that each Φ_n is a positive integer (see [16, p. 428] for $\Phi_n \in \mathbb{Z}$ and [11, p. 979] for $\Phi_n > 0$). For every prime number p, let $z(p)$ be the minimum integer $n \geq 1$ such that $p \mid F_n$. It is well known that $z(p)$ exists.

Lemma 3.1. *Let $n \geq 1$ be an integer and suppose that p is a prime factor of Φ_n. Then $n = z(p)p^v$ for some integer $v \geq 0$. Furthermore, if $v \geq 1$ and $(p, n) \neq (2, 6)$ then $p \mid\mid \Phi_n$. (Note that $2^2 \mid\mid \Phi_6 = 4$.)*

Proof. See [16, Discussion before Lemma 6]. □

Lemma 3.2. *Let $x > 1$ and $\mathcal{S} \subseteq \mathbb{N} \cap [1, x]$. Then we have*

$$\prod_{d \in \mathcal{S}} \Phi_d = R_{\mathcal{S}} \cdot \operatorname*{lcm}_{d \in \mathcal{S}} \Phi_d, \tag{4}$$

where $R_{\mathcal{S}}$ is a positive integer such that $p \leq x$ and $\nu_p(R_{\mathcal{S}}) \leq 2 \log x / \log p$ for every prime number p dividing $R_{\mathcal{S}}$. In particular, these conditions on $R_{\mathcal{S}}$ imply that $\log R_{\mathcal{S}} = O(x)$.

Proof. Let $R_{\mathcal{S}}$ be defined by (4). Clearly, $R_{\mathcal{S}}$ is a positive integer. Let p be a prime factor of $R_{\mathcal{S}}$ and let $d_1, \dots, d_m$ be all the m pairwise distinct elements of $\{d \in \mathcal{S} : p \mid \Phi_d\}$. Without loss of generality, we can assume that $\nu_p(\Phi_{d_1}) \leq \cdots \leq \nu_p(\Phi_{d_m})$. In light of Lemma 3.1, we have that $m \leq \lfloor \log x / \log p \rfloor + 1$ and $\nu_p(\Phi_{d_i}) \leq 2$ for every integer $i \in [1, m)$. Therefore,

$$1 \leq \nu_p(R_{\mathcal{S}}) = \sum_{i \leq m} \nu_p(\Phi_{d_i}) - \max_{i \leq m} \nu_p(\Phi_{d_i}) = \sum_{i < m} \nu_p(\Phi_{d_i}) \leq 2(m-1) \leq \frac{2 \log x}{\log p}.$$

In particular, it must be $m \geq 2$, so that Lemma 3.1 yields $p \leq x$. Finally,

$$\log R_{\mathcal{S}} \leq \log \prod_{p \leq x} p^{2 \log x / \log p} = \#\{p : p \leq x\} \cdot 2 \log x = O(x),$$

since the number of primes not exceeding x is $O(x / \log x)$. □

Lemma 3.3. *We have $\log \Phi_n = \varphi(n) \log \alpha + O(1)$, for all integers $n \geq 1$.*

Proof. See [11, Lemma 2.1(iii)]. □

For all integers $a, n \geq 1$, let us define

$$\mathcal{D}_a(n) := \{d \in \mathbb{N} : d \mid an,\ (an/d, a) = 1\}. \tag{5}$$

Note that $\mathcal{D}_1(n)$ is the set of positive divisors of n. Moreover, we have the following:

Lemma 3.4. *We have $\mathcal{D}_{ap}(n) = \mathcal{D}_a(pn) \setminus \mathcal{D}_a(n)$, for all integers $a, n \geq 1$ and for every prime number p not dividing a.*

Proof. On the one hand, if $d \in \mathcal{D}_{ap}(n)$ then $d \mid apn$ and $(apn/d, ap) = 1$. Hence, $(apn/d, a) = 1$, which implies $d \in \mathcal{D}_a(pn)$, and $d \nmid an$, which implies $d \notin \mathcal{D}_a(n)$. Thus $d \in \mathcal{D}_a(pn) \setminus \mathcal{D}_a(n)$.

On the other hand, if $d \in \mathcal{D}_a(pn) \setminus \mathcal{D}_a(n)$ then $d \mid apn$, $(apn/d, a) = 1$, and $d \nmid an$. Hence, $(apn/d, ap) = 1$ and consequently $d \in \mathcal{D}_{ap}(n)$. □

Lemma 3.5. *We have*

$$F_n = \prod_{d \,\in\, \mathcal{D}_1(n)} \Phi_d, \quad L_n = \prod_{d \,\in\, \mathcal{D}_2(n)} \Phi_d, \quad \frac{F_{3n}}{F_n} = \prod_{d \,\in\, \mathcal{D}_3(n)} \Phi_d, \quad \frac{L_{3n}}{L_n} = \prod_{d \,\in\, \mathcal{D}_6(n)} \Phi_d,$$

for all integers $n \geq 1$.

Proof. The four identities follow from (2), (3), and the fact that $\mathcal{D}_2(n) = \mathcal{D}_1(2n)/\mathcal{D}_1(n)$, $\mathcal{D}_3(n) = \mathcal{D}_1(3n)/\mathcal{D}_1(n)$, and $\mathcal{D}_6(n) = \mathcal{D}_2(3n)/\mathcal{D}_2(n)$, as consequence of Lemma 3.4. □

The next lemma belong to the folkore and makes possible to write shifted Lucas numbers as products or ratios of Fibonacci and Lucas numbers.

Lemma 3.6. *We have*

$$\begin{aligned} L_{4k} - 1 &= L_{6k}/L_{2k}, & L_{4k} + 1 &= F_{6k}/F_{2k}, \\ L_{4k+1} - 1 &= 5F_{2k}F_{2k+1}, & L_{4k+1} + 1 &= L_{2k}L_{2k+1}, \\ L_{4k+2} - 1 &= F_{6k+3}/F_{2k+1}, & L_{4k+2} + 1 &= L_{6k+3}/L_{2k+1}, \\ L_{4k+3} - 1 &= L_{2k+1}L_{2k+2}, & L_{4k+3} + 1 &= 5F_{2k+1}F_{2k+2}, \end{aligned}$$

for all integers $k \geq 1$.

Proof. Taking into account that $\alpha + \beta = 1$, $\alpha - \beta = \sqrt{5}$, and $\alpha\beta = -1$, the eight identities follow by substituting $(X, Y) = \left(\alpha^{2k}, \pm\beta^{2k}\right)$ and $(X, Y) = \left(\alpha^{2k+1}, \pm\beta^{2k+1}\right)$ into

$$\begin{aligned} X^2 + Y^2 + XY &= (X^3 - Y^3)/(X - Y), \\ \alpha X^2 + \beta Y^2 + XY &= (X + Y)(\alpha X + \beta Y), \end{aligned}$$

and using the Binet formulas (2). □

Now define the sets $(\mathcal{E}_\pm(n))_{n\geq 4}$ and the integers $(e_\pm(n))_{n\geq 4}$ by

$$\begin{aligned} \mathcal{E}_-(4k) &= \mathcal{D}_6(2k), & \mathcal{E}_+(4k) &= \mathcal{D}_3(2k), \\ \mathcal{E}_-(4k+1) &= \mathcal{D}_1(2k) \cup \mathcal{D}_1(2k+1), & \mathcal{E}_+(4k+1) &= \mathcal{D}_2(2k) \cup \mathcal{D}_2(2k+1), \\ \mathcal{E}_-(4k+2) &= \mathcal{D}_3(2k+1), & \mathcal{E}_+(4k+2) &= \mathcal{D}_6(2k+1), \\ \mathcal{E}_-(4k+3) &= \mathcal{D}_2(2k+1) \cup \mathcal{D}_2(2k+2), & \mathcal{E}_+(4k+3) &= \mathcal{D}_1(2k+1) \cup \mathcal{D}_1(2k+2), \end{aligned}$$

and $e_-(4k+1) = e_+(4k+3) = 5$, for every integer $k \geq 1$; while $e_\pm(n) = 1$ for all the other integers $n \geq 4$.

Lemma 3.7. *We have*

$$L_n + s = e_s(n) \prod_{d \,\in\, \mathcal{E}_s(n)} \Phi_d,$$

for all integers $n \geq 4$ and for all $s \in \{-1, +1\}$.

Proof. Noticing that $\mathcal{D}_1(m) \cap \mathcal{D}_1(m+1) = \{1\}$ and $\mathcal{D}_2(m) \cap \mathcal{D}_2(m+1) = \varnothing$, for every integer $m \geq 1$, the claim follows from Lemma 3.5 and Lemma 3.6. □

4. Further preliminaries

For every sequence $\mathbf{s} = (s_k)_{k \geq 1}$ in $\{-1, +1\}$ and for all integer $n \geq 4$, let us define

$$\ell_{\mathbf{s}}(n) := \operatorname*{lcm}_{4 \leq k \leq n} (L_k + s_k) \quad \text{and} \quad \mathcal{L}_{\mathbf{s}}(n) := \bigcup_{a \in \{1,2,3,6\}} \bigcup_{h \in \mathcal{K}_{a,\mathbf{s}}(n)} \mathcal{D}_a(h),$$

where

$$\begin{aligned}
\mathcal{K}_{1,\mathbf{s}}(n) &:= \big\{h \leq n/2 : s_{2h-1} = (-1)^h \vee s_{2h+1} = (-1)^{h+1}\big\}, \\
\mathcal{K}_{2,\mathbf{s}}(n) &:= \big\{h \leq n/2 : s_{2h-1} = (-1)^{h+1} \vee s_{2h+1} = (-1)^{h}\big\}, \\
\mathcal{K}_{3,\mathbf{s}}(n) &:= \big\{h \leq n/2 : s_{2h} = (-1)^h\big\}, \\
\mathcal{K}_{6,\mathbf{s}}(n) &:= \big\{h \leq n/2 : s_{2h} = (-1)^{h+1}\big\}.
\end{aligned}$$

The next lemma will be fundamental in the proofs of Theorem 1.3 and Theorem 1.4.

Lemma 4.1. *We have*

$$\log \ell_{\mathbf{s}}(n) = \sum_{d \in \mathcal{L}_{\mathbf{s}}(n)} \varphi(d) \log \alpha + O(n), \tag{6}$$

for all integers $n \geq 4$ and for all sequences $\mathbf{s} = (s_k)_{k \geq 1}$ in $\{-1, +1\}$.

Proof. From the definition of $\mathcal{E}_{\pm}(k)$, it follows that the symmetric difference of $\mathcal{L}_{\mathbf{s}}(n)$ and

$$\mathcal{L}'_{\mathbf{s}}(n) := \bigcup_{4 \leq k \leq n} \mathcal{E}_{s_k}(k)$$

is contained in $[1, 4] \cup \big[(n-1)/2, (n+1)/2\big]$. Therefore, it suffices to prove (6) with $\mathcal{L}'_{\mathbf{s}}(n)$ in place of $\mathcal{L}_{\mathbf{s}}(n)$.

For every integer $m \geq 1$, write $m = m^{(\leq)} \cdot m^{(>)}$, where $m^{(\leq)}$, respectively $m^{(>)}$, is a positive integer having all prime factors not exceeding $3n$, respectively greater than $3n$. Note that for every integer $k \in [4, n]$ we have $\mathcal{E}_{\pm}(k) \subseteq [1, 3n]$, and consequently $\mathcal{L}'_{\mathbf{s}}(n) \subseteq [1, 3n]$.

On the one hand, from Lemma 3.7 and Lemma 3.2 (with $x = 3n$), we have that

$$\begin{aligned}
\ell_{\mathbf{s}}^{(>)}(n) &= \operatorname*{lcm}_{4 \leq k \leq n} (L_k + s_k)^{(>)} = \operatorname*{lcm}_{4 \leq k \leq n} \prod_{d \in \mathcal{E}_{s_k}(k)} \Phi_d^{(>)} \\
&= \operatorname*{lcm}_{4 \leq k \leq n} \operatorname*{lcm}_{d \in \mathcal{E}_{s_k}(k)} \Phi_d^{(>)} = \operatorname*{lcm}_{d \in \mathcal{L}'_{\mathbf{s}}(n)} \Phi_d^{(>)} = \prod_{d \in \mathcal{L}'_{\mathbf{s}}(n)} \Phi_d^{(>)},
\end{aligned} \tag{7}$$

and

$$\prod_{d \in \mathcal{L}'_{\mathbf{s}}(n)} \Phi_d^{(\leq)} = \mathrm{e}^{O(n)}. \tag{8}$$

On the other hand, again from Lemma 3.7 and Lemma 3.2, we get that

$$\ell_{\mathbf{s}}^{(\leq)}(n) = \operatorname*{lcm}_{4 \leq k \leq n} (L_k + s_k)^{(\leq)} = \operatorname*{lcm}_{4 \leq k \leq n} \prod_{d \in \mathcal{E}_{s_k}(k)} \Phi_d^{(\leq)} = \operatorname*{lcm}_{4 \leq k \leq n} R_k = \mathrm{e}^{O(n)}, \tag{9}$$

where each R_k is a positive integer such that $p \leq 3n$ and $\nu_p(R_k) \leq 2\log(3n)/\log p$ for every prime number p dividing R_k.

Therefore, from (7), (8), and (9), we find that

$$\log \ell_{\mathbf{s}}(n) = \log\Bigg(\prod_{d \in \mathcal{L}'_{\mathbf{s}}(n)} \Phi_d\Bigg) + O(n) = \sum_{d \in \mathcal{L}'_{\mathbf{s}}(n)} \varphi(d) \log \alpha + O\big(\#\mathcal{L}'_{\mathbf{s}}(n)\big) + O(n),$$

where we used Lemma 3.3. Since $\#\mathcal{L}'_{\mathbf{s}}(n) \leq 3n$, the claim follows. ∎

For all integers $r, m \geq 1$ and for every $x > 1$, let us define the arithmetic progression

$$\mathcal{A}_{r,m}(x) := \big\{n \leq x : n \equiv r \pmod m\big\},$$

and put

$$c_{r,m} := \frac{1}{m} \prod_{\substack{p \,|\, m \\ p \,|\, r}} \left(1 + \frac{1}{p}\right)^{-1} \prod_{\substack{p \,|\, m \\ p \,\nmid\, r}} \left(1 - \frac{1}{p^2}\right)^{-1}.$$

Also, for every integer $q \geq 1$ and for all $z, w \in [0, 1]$, let us define

$$T_q(z,w) := \begin{cases} 1 & \text{if } z = 0; \\ \frac{(1-z)\operatorname{Li}_2(z)}{z} & \text{if } z > 0 \text{ and } w = 1; \\ \frac{(1-zw)\operatorname{Li}_2(z^q w)}{q^2 zw} + \frac{1-z}{z}\sum_{j=1}^{q-1} z^j \left(\frac{1}{j^2} + \frac{\operatorname{Li}_2(z^q w; j/q)}{q^2}\right) & \text{if } z > 0 \text{ and } w < 1. \end{cases}$$

We need some asymptotic formulas for sums of the Euler totient function over $\mathcal{A}_{r,m}(x)$.

Lemma 4.2. *Let $r, m, q \geq 1$ be integers, and let $z, w \in [0, 1]$. Then we have*

$$\sum_{n \,\in\, \mathcal{A}_{r,m}(x)} \varphi(n) \left(1 - z^{\lfloor \frac{x}{n} \rfloor} w^{\lfloor \frac{x}{qn} \rfloor}\right) = \frac{3}{\pi^2} c_{r,m} T_q(z,w) x^2 + O_{r,m}\big(x(\log x)^2\big),$$

for all $x \geq 2$, where for $z = 0$ the error term can be improved to $O_{r,m}(x \log x)$.

Proof. For $z = 0$, or $z > 0$ and $w = 1$, see [13, Lemma 3.4, Lemma 3.5]. Suppose that $z > 0$ and $w < 1$, and let

$$S_{r,m}(x) := \sum_{n \,\in\, \mathcal{A}_{r,m}(x)} \varphi(n) = \frac{3}{\pi^2} c_{r,m} x^2 + O_{r,m}(x \log x),$$

for all $x \geq 2$. For every integer $k \geq 1$, we have that $\lfloor x/n \rfloor = k$ if and only if $x/(k+1) < n \leq x/k$, and in such a case it holds $\lfloor x/(qn) \rfloor = \lfloor k/q \rfloor$. Therefore, we have

$$\begin{aligned}
\sum_{n \,\in\, \mathcal{A}_{r,m}(x)} \varphi(n) \left(1 - z^{\lfloor \frac{x}{n} \rfloor} w^{\lfloor \frac{x}{qn} \rfloor}\right) &= \sum_{k \,\leq\, x} \left(1 - z^k w^{\lfloor \frac{k}{q} \rfloor}\right) \left(S_{r,m}\left(\frac{x}{k}\right) - S_{r,m}\left(\frac{x}{k+1}\right)\right) \\
&= \sum_{k \,\leq\, x} \left(\left(1 - z^k w^{\lfloor \frac{k}{q} \rfloor}\right) - \left(1 - z^{k-1} w^{\lfloor \frac{k-1}{q} \rfloor}\right)\right) S_{r,m}\left(\frac{x}{k}\right) \\
&= \sum_{k \,\leq\, x} z^{k-1} \left(w^{\lfloor \frac{k-1}{q} \rfloor} - z w^{\lfloor \frac{k}{q} \rfloor}\right) \left(\frac{3}{\pi^2} \cdot \frac{c_{r,m} x^2}{k^2} + O_{r,m}\left(\frac{x \log x}{k}\right)\right) \\
&= \frac{3 c_{r,m}}{\pi^2} U_q(z,w) x^2 + O_{r,m}\left(\sum_{k \,>\, x} \frac{x^2}{k^2}\right) + O_{r,m}\left(\sum_{k \,\leq\, x} \frac{x \log x}{k}\right) \\
&= \frac{3 c_{r,m}}{\pi^2} U_q(z,w) x^2 + O_{r,m}\big(x(\log x)^2\big),
\end{aligned}$$

where

$$\begin{aligned}
U_q(z,w) &:= \sum_{k=1}^{\infty} \frac{z^{k-1}}{k^2} \left(w^{\lfloor \frac{k-1}{q} \rfloor} - z w^{\lfloor \frac{k}{q} \rfloor}\right) \\
&= (1-z) \sum_{k=1}^{q-1} \frac{z^{k-1}}{k^2} + \sum_{j=0}^{q-1} \sum_{h=1}^{\infty} \frac{z^{qh+j-1} w^h}{(qh+j)^2} \begin{cases} (w^{-1} - z) & \text{if } j = 0; \\ (1-z) & \text{if } j \geq 1; \end{cases} \\
&= \frac{(1-zw)\operatorname{Li}_2(z^q w)}{q^2 zw} + \frac{1-z}{z} \sum_{j=1}^{q-1} z^j \left(\frac{1}{j^2} + \frac{\operatorname{Li}_2(z^q w; j/q)}{q^2}\right),
\end{aligned}$$

as desired. □

5. Proof of Theorem 1.3

For all integers $a, r, m \geq 1$, let $\mathcal{T}_{a,r,m}$ be the set of $t \in \{1, \dots, m\}$ such that there exists an integer $u \geq 1$ satisfying $tu \equiv r \pmod{m}$ and $(a, u) = 1$. Moreover, for each $t \in \mathcal{T}_{a,r,m}$ let $u_{a,r,m}(t)$ be the minimum of the possible integers u.

Lemma 5.1. *Let $a, r, m \geq 1$ be integers. Then we have*

$$\bigcup_{n \in \mathcal{A}_{r,m}(x)} \mathcal{D}_a(n) = \bigcup_{t \in \mathcal{T}_{a,r,m}} \mathcal{A}_{at,am}\left(\frac{ax}{u_{a,r,m}(t)}\right),$$

for every $x > 1$.

Proof. On the one hand, suppose that $d \in \mathcal{D}_a(n)$ for some $n \in \mathcal{A}_{r,m}(x)$. In particular, $d \mid an$ and $a \mid d$. Put $u := an/d$ and let $t \in \{1, \dots, m\}$ be such that $d/a \equiv t \pmod{m}$. Then $tu \equiv (d/a)(an/d) \equiv n \equiv r \pmod{m}$ and $(a, u) = 1$, so that $t \in \mathcal{T}_{a,r,m}$. Moreover, $d \equiv at \pmod{am}$ and $d = an/u \leq ax/u_{a,r,m}(t)$, so that $d \in \mathcal{A}_{at,am}(ax/u_{a,r,m}(t))$.

On the other hand, suppose that $d \in \mathcal{A}_{at,am}(ax/u_{a,r,m}(t))$ for some $t \in \mathcal{T}_{a,r,m}$. Since $d \equiv at \pmod{am}$, we have that $a \mid d$ and $d/a \equiv t \pmod{m}$. Let $u := u_{a,r,m}(t)$ and $n := (d/a)u$. Then $d \mid an$ and $(an/d, a) = (u, a) = 1$, so that $d \in \mathcal{D}_a(n)$. Moreover, $n \equiv (d/a)u \equiv tu \equiv r \pmod{m}$ and $n \leq ((ax/u)/a)u = x$, so that $n \in \mathcal{A}_{r,m}(x)$. □

Let $\mathbf{s} = (s_n)_{n \geq 1}$ be a periodic sequence in $\{-1, +1\}$, and let m be the length of its period. Then, for each $a \in \{1, 2, 3, 6\}$, there exists $\mathcal{R}_{a,\mathbf{s}} \subseteq \{1, \dots, 2m\}$ such that

$$\mathcal{K}_{a,\mathbf{s}}(n) = \bigcup_{r \in \mathcal{R}_{a,\mathbf{s}}} \mathcal{A}_{r,2m}(n/2),$$

for all integers $n \geq 4$. From Lemma 5.1 and the fact that arithmetic progressions modulo m, $2m$, and $3m$ can be written as unions of arithmetic progressions modulo $6m$, it follows that there exist $\mathcal{R}_\mathbf{s} \subseteq \{1, \dots, 6m\}$ and positive rational numbers $(q_r)_{r \in \mathcal{R}_\mathbf{s}}$ such that

$$\mathcal{L}_\mathbf{s}(n) = \bigcup_{a \in \{1,2,3,6\}} \; \bigcup_{h \in \mathcal{K}_{a,\mathbf{s}}(n)} \mathcal{D}_a(h) = \bigcup_{r \in \mathcal{R}_\mathbf{s}} \mathcal{A}_{r,6m}(q_r n).$$

Now Lemma 4.1 and Lemma 4.2 yield that

$$\log \ell_\mathbf{s}(n) = \sum_{r \in \mathcal{R}_\mathbf{s}} \; \sum_{d \in \mathcal{A}_{r,6m}(q_r n)} \varphi(d) \log \alpha + O(n) = B_\mathbf{s} \cdot \frac{\log \alpha}{\pi^2} \cdot n^2 + O_\mathbf{s}(n \log n),$$

for all integers $n \geq 4$, where

$$B_\mathbf{s} := 3 \sum_{r \in \mathcal{R}_\mathbf{s}} c_{r,6m} q_r^2$$

is a positive rational number, which is effectively computable in terms of $s_1, \dots, s_m$.

The proof is complete.

6. Proof of Theorem 1.4

For all integers $a, d \geq 1$ and for every $x > 1$, let us define

$$\mathcal{H}_a(d) := \big\{h \in \mathbb{N} : d \in \mathcal{D}_a(h)\big\} \quad \text{and} \quad \mathcal{H}_a(d; x) := \mathcal{H}_a(d) \cap [1, x].$$

We need the following easy result.

Lemma 6.1. *For all integers $a, b, d \geq 1$ and for every $x > 1$, we have that:*

(i) If $a \mid d$ then $\mathcal{H}_a(d) = \big\{\frac{d}{a}v : v \in \mathbb{N},\ (a, v) = 1\big\}$, otherwise $\mathcal{H}_a(d) = \varnothing$.

(ii) If $a \mid d$ then $\#\mathcal{H}_a(d; x) = \sum_{b \mid a} \mu(b) \big\lfloor \frac{ax}{bd} \big\rfloor$, otherwise $\#\mathcal{H}_a(d; x) = 0$.

(iii) If $a \neq b$ then $\mathcal{H}_a(d) \cap \mathcal{H}_b(d) = \varnothing$.

Proof. The claim (i) follows easily from (5), while (ii) is a consequence of (i) and the inclusion-exclusion principle. Regarding (iii), suppose that $h \in \mathcal{H}_a(d) \cap \mathcal{H}_b(d)$. Then it follows from (i) that $h = dv/a = dw/b$, for some integers $v, w \geq 1$ such that $(a, v) = 1$ and $(b, w) = 1$. Hence, $bv = aw$ and by the conditions of coprimality it follows that $a = b$. □

In what follows, let $\mathbf{s} = (s_n)_{n\geq 1}$ be a sequence of independent and uniformly distributed random variables in $\{-1, +1\}$. Furthermore, define

$$P(d,n) := \begin{cases} 2\left\lfloor \frac{n}{2d} \right\rfloor & \text{if } d \equiv 1,5 \pmod 6; \\ 2\left\lfloor \frac{n}{d} \right\rfloor & \text{if } d \equiv 2,4 \pmod 6; \\ \left\lfloor \frac{3n}{2d} \right\rfloor + \left\lfloor \frac{n}{2d} \right\rfloor & \text{if } d \equiv 3 \pmod 6; \\ \left\lfloor \frac{3n}{d} \right\rfloor + \left\lfloor \frac{n}{d} \right\rfloor & \text{if } d \equiv 0 \pmod 6; \end{cases} \tag{10}$$

for all integers $d, n \geq 1$.

Lemma 6.2. *We have*

$$\mathbb{P}\big[d \in \mathcal{L}_{\mathbf{s}}(n)\big] = 1 - \left(\tfrac{1}{2}\right)^{P(d,n)},$$

for all integers $n \geq 4$ and $d \geq 12$.

Proof. Let $a_1, a_2 \in \{1, 2, 3, 6\}$ and $h_i \in \mathcal{H}_{a_i}(d)$, for $i = 1, 2$, with $(a_1, h_1) \neq (a_2, h_2)$. By Lemma 6.1(iii) we have that $h_1 \neq h_2$. Moreover, by Lemma 6.1(i) and $d \geq 12$, we have that

$$2 \leq \frac{d}{6} \leq \frac{d}{(a_1, a_2)} = \left(\frac{d}{a_1}, \frac{d}{a_2}\right) \mid h_1 - h_2.$$

Hence, $|h_1 - h_2| \geq 2$ and consequently

$$\{2h_1 - 1, 2h_1, 2h_1 + 1\} \cap \{2h_2 - 1, 2h_2, 2h_2 + 1\} = \varnothing.$$

Therefore, the events $\big(h \notin \mathcal{K}_{a,\mathbf{s}}(n)\big)$, with $a \in \{1, 2, 3, 6\}$ and $h \in \mathcal{H}_a(d)$, are mutually independent. Moreover, we have

$$\mathbb{P}\big[h \notin \mathcal{K}_{1,\mathbf{s}}(n)\big] = \mathbb{P}\big[h \notin \mathcal{K}_{2,\mathbf{s}}(n)\big] = \tfrac{1}{4} \quad \text{and} \quad \mathbb{P}\big[h \notin \mathcal{K}_{3,\mathbf{s}}(n)\big] = \mathbb{P}\big[h \notin \mathcal{K}_{6,\mathbf{s}}(n)\big] = \tfrac{1}{2}.$$

Thus it follows that

$$\begin{aligned} \mathbb{P}\big[d \notin \mathcal{L}_{\mathbf{s}}(n)\big] &= \mathbb{P}\Bigg[\bigwedge_{a \in \{1,2,3,6\}} \bigwedge_{h \in \mathcal{K}_{a,\mathbf{s}}(n)} \big(d \notin \mathcal{D}_a(h)\big)\Bigg] \\ &= \mathbb{P}\Bigg[\bigwedge_{a \in \{1,2,3,6\}} \bigwedge_{h \in \mathcal{H}_a(d;n/2)} \big(h \notin \mathcal{K}_{a,\mathbf{s}}(n)\big)\Bigg] \\ &= \prod_{a \in \{1,2,3,6\}} \prod_{h \in \mathcal{H}_a(d;n/2)} \mathbb{P}\big[h \notin \mathcal{K}_{a,\mathbf{s}}(n)\big] \\ &= \left(\tfrac{1}{4}\right)^{\#\mathcal{H}_1(d,n/2)} \left(\tfrac{1}{4}\right)^{\#\mathcal{H}_2(d,n/2)} \left(\tfrac{1}{2}\right)^{\#\mathcal{H}_3(d,n/2)} \left(\tfrac{1}{2}\right)^{\#\mathcal{H}_6(d,n/2)} = \left(\tfrac{1}{2}\right)^{P(d,n)}, \end{aligned}$$

where the last equality follows by Lemma 6.1(ii) and (10). □

We are ready to prove Theorem 1.4. From Lemma 4.1 and Lemma 6.2, we have that

$$\mathbb{E}\left[\frac{\log \ell_{\mathbf{s}}(n)}{\log \alpha}\right] = \sum_{d \leq 3n} \varphi(d)\, \mathbb{P}\big[d \in \mathcal{L}_{\mathbf{s}}(n)\big] + O(n) = \sum_{d \leq 3n} \varphi(d) \left(1 - \left(\tfrac{1}{2}\right)^{P(d,n)}\right) + O(n),$$

for every sufficiently large integer n. Let S be the last sum. Splitting S according to the residue class of d modulo 6, and applying Lemma 4.2, we get

$$\begin{aligned} S = &\sum_{d \in \mathcal{A}_{1,6}(n/2) \cup \mathcal{A}_{5,6}(n/2)} \varphi(d) \left(1 - \left(\tfrac{1}{4}\right)^{\left\lfloor \frac{n}{2d} \right\rfloor}\right) + \sum_{d \in \mathcal{A}_{2,6}(n) \cup \mathcal{A}_{4,6}(n)} \varphi(d) \left(1 - \left(\tfrac{1}{4}\right)^{\left\lfloor \frac{n}{d} \right\rfloor}\right) \\ &+ \sum_{d \in \mathcal{A}_{3,6}(3n/2)} \varphi(d) \left(1 - \left(\tfrac{1}{2}\right)^{\left\lfloor \frac{3n}{2d} \right\rfloor + \left\lfloor \frac{n}{2d} \right\rfloor}\right) + \sum_{d \in \mathcal{A}_{6,6}(3n)} \varphi(d) \left(1 - \left(\tfrac{1}{2}\right)^{\left\lfloor \frac{3n}{d} \right\rfloor + \left\lfloor \frac{n}{d} \right\rfloor}\right) \end{aligned}$$

$$= \Big(\tfrac{9}{8}\operatorname{Li}_2\big(\tfrac{1}{4}\big) + \tfrac{9}{4}\operatorname{Li}_2\big(\tfrac{1}{4}\big) + \Big(\tfrac{81}{128} + \tfrac{3}{8}\operatorname{Li}_2\big(\tfrac{1}{16}\big) + \tfrac{1}{16}\operatorname{Li}_2\big(\tfrac{1}{16};\tfrac{1}{3}\big) + \tfrac{1}{32}\operatorname{Li}_2\big(\tfrac{1}{16};\tfrac{2}{3}\big)\Big)$$
$$+ \Big(\tfrac{81}{64} + \tfrac{3}{4}\operatorname{Li}_2\big(\tfrac{1}{16}\big) + \tfrac{1}{8}\operatorname{Li}_2\big(\tfrac{1}{16};\tfrac{1}{3}\big) + \tfrac{1}{16}\operatorname{Li}_2\big(\tfrac{1}{16};\tfrac{2}{3}\big)\Big)\Big)\frac{n^2}{\pi^2} + O\big(n(\log n)^2\big)$$
$$= C \cdot \frac{n^2}{\pi^2} + O\big(n(\log n)^2\big)\,.$$

The proof is complete.

References

1. S. Akiyama, *Lehmer numbers and an asymptotic formula for* π, J. Number Theory **36** (1990), no. 3, 328–331.
2. S. Akiyama, *A new type of inclusion exclusion principle for sequences and asymptotic formulas for* $\zeta(k)$, J. Number Theory **45** (1993), no. 2, 200–214.
3. S. Akiyama, *A criterion to estimate the least common multiple of sequences and asymptotic formulas for* $\zeta(3)$ *arising from recurrence relation of an elliptic function*, Japan. J. Math. (N.S.) **22** (1996), no. 1, 129–146.
4. S. Akiyama and F. Luca, *On the least common multiple of Lucas subsequences*, Acta Arith. **161** (2013), no. 4, 327–349.
5. G. Alsmeyer, Z. Kabluchko, and A. Marynych, *Limit theorems for the least common multiple of a random set of integers*, Trans. Amer. Math. Soc. **372** (2019), no. 7, 4585–4603.
6. J.-P. Bézivin, *Plus petit commun multiple des termes consécutifs d'une suite récurrente linéaire*, Collect. Math. **40** (1989), no. 1, 1–11 (1990).
7. J. Cilleruelo, J. Rué, P. Šarka, and A. Zumalacárregui, *The least common multiple of random sets of positive integers*, J. Number Theory **144** (2014), 92–104.
8. J. P. Jones and P. Kiss, *An asymptotic formula concerning Lehmer numbers*, Publ. Math. Debrecen **42** (1993), no. 3-4, 199–213.
9. P. Kiss and F. Mátyás, *An asymptotic formula for* π, J. Number Theory **31** (1989), no. 3, 255–259.
10. Y. V. Matiyasevich and R. K. Guy, *A new formula for* π, Amer. Math. Monthly **93** (1986), no. 8, 631–635.
11. C. Sanna, *Practical numbers in Lucas sequences*, Quaest. Math. **42** (2019), no. 7, 977–983.
12. C. Sanna, *On the l.c.m. of random terms of binary recurrence sequences*, J. Number Theory **213** (2020), 221–231.
13. C. Sanna, *On the l.c.m. of shifted Fibonacci numbers*, Int. J. Number Theory (2021), Online ready: https://doi.org/10.1142/S1793042121500743.
14. C. Sanna, *On the least common multiple of random q-integers*, Res. Number Theory **7** (2021), no. 1, Paper No. 16, 10.
15. C. Sanna, *On the least common multiple of shifted powers*, J. Integer Seq. **24** (2021), no. 7, Article 21.7.3.
16. C. L. Stewart, *On divisors of Fermat, Fibonacci, Lucas, and Lehmer numbers*, Proc. London Math. Soc. (3) **35** (1977), no. 3, 425–447.
17. B. Tropak, *Some asymptotic properties of Lucas numbers*, Proceedings of the Regional Mathematical Conference (Kalsk, 1988), Pedagog. Univ. Zielona Góra, Zielona Góra, 1990, pp. 49–55.

Politecnico di Torino, Department of Mathematical Sciences
Corso Duca degli Abruzzi 24, 10129 Torino, Italy
Email address: carlo.sanna.dev@gmail.com