Journal of Integer Sequences, Vol. 24 (2021),
Article 21.7.3

On the Least Common Multiple of Shifted Powers

Carlo Sanna
Politecnico di Torino
Department of Mathematical Sciences
Corso Duca degli Abruzzi 24
10129 Torino
Italy
carlo.sanna.dev@gmail.com

Abstract

We determine the asymptotic behavior of $\log \operatorname{lcm}(a + s_1, a^2 + s_2, \ldots, a^n + s_n)$, for $a \geq 2$ an integer and $(s_n)_{n\geq 1}$ 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 $\{-1, +1\}$.

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 $n \geq 1$. Matiyasevich and Guy [10] proved that

$$\log \operatorname{lcm}(F_1, F_2, \ldots, F_n) \sim \frac{3 \log\left(\frac{1+\sqrt{5}}{2}\right)}{\pi^2} \cdot n^2,$$

as $n \to +\infty$, where lcm denotes the least common multiple. This result was generalized to Lucas sequences, Lehmer sequences, and other sequences with special divisibility properties [1–4, 6, 8, 9, 16]. In particular, for every integer $a \geq 2$ we have

$$\log \operatorname{lcm}(a - 1, a^2 - 1, \ldots, a^n - 1) \sim \frac{3 \log a}{\pi^2} \cdot n^2 \tag{1}$$

and

$$\log \operatorname{lcm}(a+1, a^2+1, \ldots, a^n+1) \sim \frac{4\log a}{\pi^2} \cdot n^2, \tag{2}$$

as $n \to +\infty$. Precisely, (1) follows from [9, Lemma 3] applied to the Lucas sequence $\left(\frac{a^n-1}{a-1}\right)_{n\geq 1}$, while (2) follows from [6, Théorème] applied to the companion Lucas sequence $(a^n+1)_{n\geq 1}$.

We generalize (1) and (2) by giving asymptotic formulas for least common multiples of sequences of *shifted powers* $(a^n + s_n)_{n\geq 1}$, where $(s_n)_{n\geq 1}$ is a sequence of *shifts* in $\{-1, +1\}$. This is somehow similar to a previous work of the author [14], in which least common multiples of the sequence of shifted Fibonacci numbers $(F_n + s_n)_{n\geq 1}$ were studied.

Our first result regards periodic sequences of shifts.

Theorem 1. *Let $a \geq 2$ be an integer and let $\mathbf{s} = (s_n)_{n\geq 1}$ be a periodic sequence in $\{-1, +1\}$. Then there exists an effectively computable rational number $C_\mathbf{s} > 0$ such that*

$$\log \operatorname{lcm}(a+s_1, a^2+s_2, \ldots, a^n+s_n) \sim C_\mathbf{s} \cdot \frac{\log a}{\pi^2} \cdot n^2, \tag{3}$$

as $n \to +\infty$.

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 $C_\mathbf{s}$. Indeed, we implemented such algorithm and we computed the constant $C_\mathbf{s}$ for periodic sequences with short period, see Table 1.

$\mathbf{s}$	$C_\mathbf{s}$	$\mathbf{s}$	$C_\mathbf{s}$	$\mathbf{s}$	$C_\mathbf{s}$	$\mathbf{s}$	$C_\mathbf{s}$
−	3	−+−−	27/8	−−+−+	319/96	+−−+−	733/216
+	4	−++−	125/36	−−++−	487/144	+−−++	769/216
−+	4	−+++	38/9	−−+++	7687/2160	+−+−−	487/144
+−	3	+−−−	3	−+−−−	101/32	+−+−+	7687/2160
−−+	13/4	+−−+	7/2	−+−−+	319/96	+−++−	2123/576
−+−	105/32	+−++	7/2	−+−+−	487/144	+−+++	2219/576
−++	173/48	++−−	125/36	−+−++	7687/2160	++−−−	487/144
+−−	105/32	++−+	38/9	−++−−	733/216	++−−+	7687/2160
+−+	173/48	+++−	27/8	−++−+	769/216	++−+−	2123/576
++−	47/12	−−−−+	19/6	−+++−	2123/576	++−++	2219/576
−−−+	7/2	−−−+−	101/32	−++++	2219/576	+++−−	2123/576
−−+−	3	−−−++	319/96	+−−−−	101/32	+++−+	2219/576
−−++	7/2	−−+−−	101/32	+−−−+	319/96	++++−	39/10

Table 1: Values of $C_\mathbf{s}$ for periodic sequences $\mathbf{s}$ of period at most 5.

Our second result is an asymptotic formula for random sequences of shifts (see [5,7,12,13] for similar results on least common multiples of random sequences).

Theorem 2. *Let $a \geq 2$ be an integer and let $(s_n)_{n\geq 1}$ be a sequence of independent and uniformly distributed random variables in $\{-1, +1\}$. Then*

$$\log \operatorname{lcm}(a + s_1, a^2 + s_2, \dots, a^n + s_n) \sim 6 \operatorname{Li}_2\!\left(\tfrac{1}{2}\right) \cdot \frac{\log a}{\pi^2} \cdot n^2, \tag{4}$$

with probability $1 - o(1)$*, as* $n \to +\infty$*, where* $\operatorname{Li}_2(z) := \sum_{k=1}^{\infty} z^k/k^2$ *is the dilogarithm function.*

Remark 1. It is known that $\operatorname{Li}_2\!\left(\frac{1}{2}\right) = \left(\pi^2 - 6(\log 2)^2\right)/12$ (see, e.g., [17]), but in (4) we preferred to keep explicit the factor $6 \operatorname{Li}_2\!\left(\frac{1}{2}\right)$ in order to ease the comparison with (1), (2), and (3). Numerically, we have $6 \operatorname{Li}_2\!\left(\frac{1}{2}\right) = 3.493443\dots$ so that the right-hand side of (4) is a bit less than the arithmetic mean of the right-hand sides of (1) and (2).

We leave the following questions to the interested reader:

Question 1. Is there a simple characterization of the set $\mathcal{E}$ of sequences $\mathbf{s} = (s_n)_{n\geq 1}$ in $\{-1, +1\}$ such that the limit

$$L(\mathbf{s}) := \lim_{n \to +\infty} \frac{\log \operatorname{lcm}(a + s_1, a^2 + s_2, \dots, a^n + s_n)}{(\log a/\pi^2) \cdot n^2}$$

exists? (It follows from Lemma 3 below that $L(\mathbf{s})$ does not depend on a.)

Question 2. What is the image $L(\mathcal{E})$?

Question 3. Does (an appropriate normalization of) the random variable on the left-hand side of (4) converge to some known distribution?

2 Notation

We employ the Landau-Bachmann "Big Oh" and "little oh" notations O and o, as well as the associated Vinogradov symbol $\ll$, with their usual meanings. For real random variables X_n and Y_n, depending on n, we say that "$X_n \sim Y_n$ with probability $1 - o(1)$ as $n \to +\infty$" if for every $\varepsilon > 0$ we have $\mathbb{P}\big[|X_n - Y_n| > \varepsilon |Y_n|\big] = o_\varepsilon(1)$ as $n \to +\infty$. We let $[m, n]$ and (m, n) denote the least common multiple and the greatest common divisor, respectively, of the two integers m and n. We reserve the letter p for prime numbers, and we let $\nu_p(n)$ denote the p-adic valuation of the positive integer n, that is, the exponent of p in the prime factorization of n. We write $\varphi(n)$ and $\tau(n)$ for the Euler function and the number of positive divisors, respectively, of a natural number n.

3 Preliminaries

Hereafter, let $a \geq 2$ be a fixed integer. Define the *nth cyclotomic polynomial* by

$$\Phi_n(X) := \prod_{\substack{1 \leq k \leq n \\ (n,k) = 1}} \left(X - \mathrm{e}^{\frac{2\pi \mathbf{i} k}{n}}\right), \tag{5}$$

for every integer $n \geq 1$. It is well known that $\Phi_n(X) \in \mathbb{Z}[X]$. Moreover, from (5) we get that

$$a^n - 1 = \prod_{d \,\in\, \mathcal{D}^-(n)} \Phi_d(a) \quad \text{and} \quad a^n + 1 = \prod_{d \,\in\, \mathcal{D}^+(n)} \Phi_d(a), \tag{6}$$

for every integer $n \geq 1$, where $\mathcal{D}^-(n) := \{d \in \mathbb{N} : d \mid n\}$ and $\mathcal{D}^+(n) := \mathcal{D}^-(2n) \setminus \mathcal{D}^-(n)$.

We need two results about the sequence of integers $(\Phi_d(a))_{d\in\mathbb{N}}$.

Lemma 1. *We have $(\Phi_m(a), \Phi_n(a)) \mid m$, for all integers $m > n \geq 1$.*

Proof. Let $d := (\Phi_m(a), \Phi_n(a))$. By (6) we have that d divides $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$. Moreover, since $(m, n) < m$, by (6) again we have that

$$d \mid \Phi_m(a) \mid \frac{a^m - 1}{a^{(m,n)} - 1} \equiv 1 + a^{(m,n)} + \left(a^{(m,n)}\right)^2 + \cdots + \left(a^{(m,n)}\right)^{\frac{m}{(m,n)} - 1} \equiv \frac{m}{(m,n)} \pmod{d}.$$

Consequently, d divides $m/(m, n)$ and, a fortiori, d divides m. □

Lemma 2. *We have $\log \Phi_n(a) = \varphi(n) \log a + O_a(1)$, for every integer $n \geq 1$.*

Proof. See [11, Lemma 2.1(iii)]. □

For every sequence $\mathbf{s} = (s_n)_{n\geq 1}$ in $\{-1, +1\}$, let us define

$$\ell_{a,\mathbf{s}}(n) := \operatorname{lcm}(a + s_1, a^2 + s_2, \ldots, a^n + s_n)$$

and

$$\mathcal{L}_{\mathbf{s}}(n) := \bigcup_{k \,\leq\, n} \mathcal{D}^{(s_k)}(k),$$

for all integers $n \geq 1$.

The next lemma will be fundamental in the proofs of Theorem 1 and Theorem 2.

Lemma 3. *We have*

$$\log \ell_{a,\mathbf{s}}(n) = \sum_{d \,\in\, \mathcal{L}_{\mathbf{s}}(n)} \varphi(d) \log a + O_a\!\left(\frac{n^2}{\log n}\right),$$

for every integer $n \geq 2$.

Proof. For every integer $m \geq 1$, write $m = m^{(\leq)} \cdot m^{(>)}$, where $m^{(\leq)}$, respectively $m^{(>)}$, is a positive integer having all the prime factors not exceeding $2n$, respectively greater than $2n$.

Suppose that $p^v \mid\mid \ell_{a,\mathbf{s}}(n)$, for some prime number $p \leq 2n$ and some integer $v \geq 1$. Then $p^v \mid a^k + s_k$ for some positive integer $k \leq n$, and consequently $p^v \leq a^{n+1}$. Therefore,

$$\begin{aligned} \log \ell_{a,\mathbf{s}}^{(\leq)}(n) &= \log\Bigg(\prod_{\substack{p^v \,\mid\mid\, \ell_{a,\mathbf{s}}(n) \\ p \,\leq\, 2n}} p^v\Bigg) \leq \log\Bigg(\prod_{\substack{p^v \,\mid\mid\, \ell_{a,\mathbf{s}}(n) \\ p \,\leq\, 2n}} a^{n+1}\Bigg) \\ &\leq \#\{p : p \leq 2n\} \cdot (n+1) \log a \ll_a \frac{n^2}{\log n}, \end{aligned} \tag{7}$$

since the number of primes not exceeding $2n$ is $O(n/\log n)$.

On the one hand, in light of Lemma 1, the integers $\Phi_1^{(>)}(a), \dots, \Phi_{2n}^{(>)}(a)$ are pairwise coprime. Hence, also using (6), we have

$$\begin{aligned} \ell_{a,\mathbf{s}}^{(>)}(n) &= \operatorname*{lcm}_{k=1,\dots,n} (a^k + s_k)^{(>)} = \operatorname*{lcm}_{k=1,\dots,n} \prod_{d \in \mathcal{D}^{(s_k)}(n)} \Phi_d^{(>)}(a) \\ &= \operatorname*{lcm}_{k=1,\dots,n} \operatorname*{lcm}_{d \in \mathcal{D}^{(s_k)}(n)} \Phi_d^{(>)}(a) = \operatorname*{lcm}_{d \in \mathcal{L}_{\mathbf{s}}(n)} \Phi_d^{(>)}(a) \mid \operatorname*{lcm}_{d \in \mathcal{L}_{\mathbf{s}}(n)} \Phi_d(a). \end{aligned} \tag{8}$$

On the other hand, using (6) again, we have

$$\begin{aligned} \operatorname*{lcm}_{d \in \mathcal{L}_{\mathbf{s}}(n)} \Phi_d(a) &= \operatorname*{lcm}_{k=1,\dots,n} \operatorname*{lcm}_{d \in \mathcal{D}^{(s_k)}(n)} \Phi_d(a) \mid \operatorname*{lcm}_{k=1,\dots,n} \prod_{d \in \mathcal{D}^{(s_k)}(n)} \Phi_d(a) \\ &= \operatorname*{lcm}_{k=1,\dots,n} (a^k + s_k) = \ell_{a,\mathbf{s}}(n). \end{aligned} \tag{9}$$

Therefore, putting together (7), (8), and (9), we get that

$$\begin{aligned} \log \ell_{a,\mathbf{s}}(n) &= \log\Big(\prod_{d \in \mathcal{L}_{\mathbf{s}}(n)} \Phi_d(a) \Big) + O\big(\log \ell_{a,\mathbf{s}}^{(\leq)}(n)\big) \\ &= \log\Big(\prod_{d \in \mathcal{L}_{\mathbf{s}}(n)} \Phi_d(a) \Big) + O_a\left(\frac{n^2}{\log n} \right) \\ &= \sum_{d \in \mathcal{L}_{\mathbf{s}}(n)} \varphi(d) \log a + O_a(\#\mathcal{L}_{\mathbf{s}}(n)) + O_a\left(\frac{n^2}{\log n} \right), \end{aligned}$$

where we used Lemma 2. The claim follows since $\mathcal{L}_{\mathbf{s}}(n) \subseteq [1, 2n]$ and so $\#\mathcal{L}_{\mathbf{s}}(n) \leq 2n$. □

For all integers $r \geq 0$ and $m \geq 1$, and for every $x \geq 1$, let us define the arithmetic progression

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

We need an asymptotic formula for a sum of the Euler totient function over an arithmetic progression.

Lemma 4. *Let r, m be positive integers and let $z \in [0, 1)$. Then we have*

$$\sum_{n \in \mathcal{A}_{r,m}(x)} \varphi(n)\big(1 - z^{\lfloor x/n \rfloor}\big) = \frac{3}{\pi^2} \cdot c_{r,m} \cdot \frac{(1-z)\operatorname{Li}_2(z)}{z} \cdot x^2 + O_{r,m}\big(x(\log x)^2\big),$$

for every $x \geq 2$, where

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

while for $z = 0$ the factor involving $\operatorname{Li}_2(z)$ is meant to be equal to 1, and the error term can be improved to $O_{r,m}(x \log x)$.

Proof. See [14, Lemma 3.4, Lemma 3.5]. □

4 Proof of Theorem 1

For all integers $r, m \geq 1$, let us define the sets

$$\mathcal{T}^-_{r,m} := \big\{t \in \{1, \dots, 2m\} : \exists v \geq 1 \text{ s.t. } tv \equiv r \pmod m\big\},$$
$$\mathcal{T}^+_{r,m} := \big\{t \in \{1, \dots, 2m\} : 2 \mid t,\ \exists v \geq 1 \text{ s.t. } 2 \nmid v \text{ and } \tfrac{t}{2}v \equiv r \pmod m\big\}$$

and the associated values

$$\theta^-_{r,m}(t) := \big(\min\{v \geq 1 : tv \equiv r \pmod m\}\big)^{-1} \qquad \text{for each } t \in \mathcal{T}^-_{r,m},$$
$$\theta^+_{r,m}(t) := 2\big(\min\{v \geq 1 : 2 \nmid v \text{ and } \tfrac{t}{2}v \equiv r \pmod m\}\big)^{-1} \qquad \text{for each } t \in \mathcal{T}^+_{r,m}.$$

The next lemma regards unions of $\mathcal{D}^-(k)$, respectively $\mathcal{D}^+(k)$, with $k \in \mathcal{A}_{r,m}(x)$.

Lemma 5. *Let $r, m \geq 1$ be integers and let $u \in \{-1, +1\}$. Then we have*

$$\bigcup_{k \in \mathcal{A}_{r,m}(x)} \mathcal{D}^{(u)}(k) = \bigcup_{t \in \mathcal{T}^{(u)}_{r,m}} \mathcal{A}_{t,2m}\big(\theta^{(u)}_{r,m}(t)x\big),$$

for every $x \geq 1$.

Proof. For $u = +1$, the claim is [14, Lemma 3.3]. For $u = -1$, the claim is [14, Lemma 3.2], taking into account that $\mathcal{A}_{t,m}(x) = \mathcal{A}_{t,2m}(x) \cup \mathcal{A}_{t+m,2m}(x)$. □

Proof of Theorem 1. Let $\mathbf{s} = (s_n)_{n\geq1}$ be a periodic sequence in $\{-1, +1\}$, and let m be the length of its period. Moreover, let $\mathcal{R}^{(u)}_{\mathbf{s}} := \{r \in \{1, \dots, m\} : s_r = u\}$ for $u \in \{-1, +1\}$.

By periodicity of $\mathbf{s}$ and by Lemma 5, it follows that

$$\begin{aligned}
\mathcal{L}_{\mathbf{s}}(n) &= \bigcup_{u \in \{-1,+1\}} \bigcup_{r \in \mathcal{R}^{(u)}_{\mathbf{s}}} \bigcup_{k \in \mathcal{A}_{r,m}(n)} \mathcal{D}^{(u)}(k) \\
&= \bigcup_{u \in \{-1,+1\}} \bigcup_{r \in \mathcal{R}^{(u)}_{\mathbf{s}}} \bigcup_{t \in \mathcal{T}^{(u)}_{r,m}} \mathcal{A}_{t,2m}\big(\theta^{(u)}_{r,m}(t)n\big) \\
&= \bigcup_{t \in \mathcal{T}_{\mathbf{s}}} \mathcal{A}_{t,2m}\big(\theta_{\mathbf{s}}(t)n\big)
\end{aligned}$$

where

$$\mathcal{T}_{\mathbf{s}} := \bigcup_{u \in \{-1,+1\}} \bigcup_{r \in \mathcal{R}^{(u)}_{\mathbf{s}}} \mathcal{T}^{(u)}_{r,m} = \bigcup_{r=1}^{m} \mathcal{T}^{(s_r)}_{r,m}$$

and

$$\theta_{\mathbf{s}}(t) := \max\big\{\theta^{(u)}_{r,m}(t) : t \in \mathcal{T}^{(u)}_{r,m} \text{ for some } u \in \{-1,+1\},\ r \in \mathcal{R}^{(u)}_{\mathbf{s}}\big\}.$$

Hence, from Lemma 3 and Lemma 4 (with $z = 0$), we get that

$$\begin{aligned}\log \ell_{a,\mathbf{s}}(n) &= \sum_{t \in \mathcal{T}_\mathbf{s}} \sum_{d \in \mathcal{A}_{t,2m}(\theta_\mathbf{s}(t)n)} \varphi(d) \log a + O_a\!\left(\frac{n^2}{\log n}\right) \\ &= C_\mathbf{s} \cdot \frac{\log a}{\pi^2} \cdot n^2 + O_{a,m}\!\left(\frac{n^2}{\log n}\right),\end{aligned}$$

where

$$C_\mathbf{s} := 3 \sum_{t \in \mathcal{T}_\mathbf{s}} c_{t,2m} \theta_\mathbf{s}(t)^2$$

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

Example 1. Let $\mathbf{s}$ be the periodic sequence with period $-1, +1, +1, +1$ of length $m = 4$. We have

$$\begin{aligned}
&\mathcal{T}_{1,4}^- = \{1,3,5,7\}, && \theta_{1,4}^-(1) = 1, \quad \theta_{1,4}^-(3) = \tfrac{1}{3}, \quad \theta_{1,4}^-(5) = 1, \quad \theta_{1,4}^-(7) = \tfrac{1}{3}, \\
&\mathcal{T}_{2,4}^+ = \{4\}, && \theta_{2,4}^+(4) = 2, \\
&\mathcal{T}_{3,4}^+ = \{2,6\}, && \theta_{3,4}^+(2) = \tfrac{2}{3}, \quad \theta_{3,4}^+(6) = 2, \\
&\mathcal{T}_{4,4}^+ = \{8\}, && \theta_{4,4}^+(8) = 2,
\end{aligned}$$

so that $\mathcal{T}_\mathbf{s} = \{1,2,3,4,5,6,7,8\}$ and

$$\begin{aligned}
&\theta_\mathbf{s}(1) = 1, && \theta_\mathbf{s}(2) = \tfrac{2}{3}, && \theta_\mathbf{s}(3) = \tfrac{1}{3}, && \theta_\mathbf{s}(4) = 2, \\
&\theta_\mathbf{s}(5) = 1, && \theta_\mathbf{s}(6) = 2, && \theta_\mathbf{s}(7) = \tfrac{1}{3}, && \theta_\mathbf{s}(8) = 2.
\end{aligned}$$

Moreover, $c_{r,8} = \frac{1}{6}$ if r is odd, and $c_{r,8} = \frac{1}{12}$ if r is even. Therefore, we have

$$C_\mathbf{s} = 3 \cdot \Big(\tfrac{1}{6} \cdot 1^2 + \tfrac{1}{12} \cdot \big(\tfrac{2}{3}\big)^2 + \tfrac{1}{6} \cdot \big(\tfrac{1}{3}\big)^2 + \tfrac{1}{12} \cdot 2^2 + \tfrac{1}{6} \cdot 1^2 + \tfrac{1}{12} \cdot 2^2 + \tfrac{1}{6} \cdot \big(\tfrac{1}{3}\big)^2 + \tfrac{1}{12} \cdot 2^2\Big) = \tfrac{38}{9}.$$

5 Proof of Theorem 2

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

$$I_\mathbf{s}(n,d) := \begin{cases} 1, & \text{if } d \in \mathcal{L}_\mathbf{s}(n); \\ 0, & \text{otherwise,} \end{cases}$$

for all integers $n, d \geq 1$. The next lemma gives two expected values involving $I_\mathbf{s}(n,d)$.

Lemma 6. *We have*

$$\mathbb{E}\big[I_\mathbf{s}(n,d)\big] = 1 - 2^{-\lfloor n(2,d)/d \rfloor} \tag{10}$$

and

$$\mathbb{E}\big[I_{\mathbf{s}}(n,d_1)I_{\mathbf{s}}(n,d_2)\big] = 1 - 2^{-\lfloor n(2,d_1)/d_1\rfloor} - 2^{-\lfloor n(2,d_2)/d_2\rfloor} \\ + 2^{-\lfloor n(2,d_1)/d_1\rfloor - \lfloor n(2,d_2)/d_2\rfloor + \lfloor n(2,[d_1,d_2])/[d_1,d_2]\rfloor} \begin{cases} 1, & \text{if } \nu_2(d_1) = \nu_2(d_2); \\ 0, & \text{otherwise,} \end{cases}$$

for all integers $d, d_1, d_2 \geq 1$.

Proof. On the one hand, by the definitions of $I_{\mathbf{s}}(n,d)$ and $\mathcal{L}_{\mathbf{s}}(n)$, we have

$$\begin{aligned} \mathbb{E}\big[I_{\mathbf{s}}(n,d)\big] &= \mathbb{P}\big[d \in \mathcal{L}_{\mathbf{s}}(n)\big] = 1 - \mathbb{P}\Bigg[\bigwedge_{k \leq n} \big(d \notin \mathcal{D}^{(s_k)}(k)\big)\Bigg] = 1 - \mathbb{P}\Bigg[\bigwedge_{\substack{k \leq n \\ d \,|\, 2k}} \big(d \notin \mathcal{D}^{(s_k)}(k)\big)\Bigg] \\ &= 1 - \mathbb{P}\Bigg[\bigwedge_{\substack{k \leq n \\ d \,|\, 2k}} \big((d \mid k \wedge s_k = +1) \vee (d \nmid k \wedge s_k = -1)\big)\Bigg] = 1 - 2^{-\#\{k \leq n \,:\, d \,|\, 2k\}} \\ &= 1 - 2^{-\lfloor n(2,d)/d\rfloor}, \end{aligned}$$

which is (10).

On the other hand, by linearity of the expectation and by (10), we have

$$\begin{aligned} \mathbb{E}\big[I_{\mathbf{s}}(n,d_1)I_{\mathbf{s}}(n,d_2)\big] &= \mathbb{E}\big[I_{\mathbf{s}}(n,d_1) + I_{\mathbf{s}}(n,d_2) - 1 + \big(1 - I_{\mathbf{s}}(n,d_1)\big)\big(1 - I_{\mathbf{s}}(n,d_2)\big)\big] \\ &= \mathbb{E}\big[I_{\mathbf{s}}(n,d_1)\big] + \mathbb{E}\big[I_{\mathbf{s}}(n,d_2)\big] - 1 + \mathbb{E}\big[\big(1 - I_{\mathbf{s}}(n,d_1)\big)\big(1 - I_{\mathbf{s}}(n,d_2)\big)\big] \\ &= 1 - 2^{-\lfloor n(2,d_1)/d_1\rfloor} - 2^{-\lfloor n(2,d_2)/d_2\rfloor} + \mathbb{P}\big[d_1 \notin \mathcal{L}_{\mathbf{s}}(n) \wedge d_2 \notin \mathcal{L}_{\mathbf{s}}(n)\big]. \end{aligned} \quad (11)$$

Let P be the probability at the end of (11).

Suppose for a moment that $[d_1, d_2] \leq 2n$ and that d_1 and d_2 have different 2-adic valuations, say $\nu_2(d_1) < \nu_2(d_2)$, without loss of generality. Let $h := [d_1, d_2]/2$ and note that h is an integer not exceeding n. Furthermore, $d_1 \in \mathcal{D}^{-}(h)$ and $d_2 \in \mathcal{D}^{+}(h)$. Hence, no matter the value of s_h, at least one of d_1, d_2 belongs to $\mathcal{L}_{\mathbf{s}}(n)$, and consequently $P = 0$.

Now suppose that $[d_1, d_2] > 2n$ or $\nu_2(d_1) = \nu_2(d_2)$. In the second case, note that for every integer k such that $[d_1, d_2] \mid 2k$ we have that either $d_1 \mid k$ and $d_2 \mid k$, or $d_1 \nmid k$ and $d_2 \nmid k$.

Therefore,

$$
\begin{aligned}
P = \mathbb{P}\Bigg[&\bigwedge_{\substack{k \le n \\ d_1 \,|\, 2k \,\wedge\, d_2 \nmid 2k}} \big((d_1 \mid k \wedge s_k = +1) \vee (d_1 \nmid k \wedge s_k = -1)\big) \\
&\wedge \bigwedge_{\substack{k \le n \\ d_1 \nmid 2k \,\wedge\, d_2 \,|\, 2k}} \big((d_2 \mid k \wedge s_k = +1) \vee (d_2 \nmid k \wedge s_k = -1)\big) \\
&\wedge \bigwedge_{\substack{k \le n \\ d_1 \,|\, 2k \,\wedge\, d_2 \,|\, 2k}} \big((d_1 \mid k \wedge d_2 \mid k \wedge s_k = +1) \vee (d_1 \nmid k \wedge d_2 \nmid k \wedge s_k = -1)\big)\Bigg] \\
&= 2^{-\#\{k \le n \,:\, d_1 \,|\, 2k \,\vee\, d_2 \,|\, 2k\}} \\
&= 2^{-\lfloor n(2,d_1)/d_1 \rfloor - \lfloor n(2,d_2)/d_2 \rfloor + \lfloor n(2,[d_1,d_2])/[d_1,d_2] \rfloor},
\end{aligned}
$$

and the proof is complete. □

The following lemma is a simple upper bound for a sum of greatest common divisors.

Lemma 7. *We have*

$$\sum_{[d_1,\, d_2] \,\le\, n} (d_1, d_2) \ll n^2,$$

for every integer $n \geq 1$.

Proof. Let $a_i := d_i/d$ for $i = 1, 2$, where $d := (d_1, d_2)$. Then we have

$$
\begin{aligned}
\sum_{[d_1,\, d_2] \,\le\, n} (d_1, d_2) &= \sum_{d \,\le\, n} d \sum_{\substack{a_1 a_2 \,\le\, n/d \\ (a_1,\, a_2) \,=\, 1}} 1 \le \sum_{d \,\le\, n} d \sum_{m \,\le\, n/d} \tau(m) \\
&\ll n \sum_{d \,\le\, n} \log\!\left(\frac{n}{d}\right) = n\,(n \log n - \log(n!)) < n^2,
\end{aligned}
$$

where we used the upper bound $\sum_{m \le x} \tau(m) \ll x \log x$ (see, e.g., [15, Ch. I.3, Theorem 3.2]) and the inequality $n! > (n/\mathrm{e})^n$. □

Proof of Theorem 2. Let us define the random variable

$$X := \sum_{d \,\le\, 2n} \varphi(d)\, I_{\mathbf{s}}(n, d).$$

From the linearity of expectation, Lemma 6, and Lemma 4, it follows that

$$\begin{aligned}
\mathbb{E}[X] &:= \sum_{d \le 2n} \varphi(d)\, \mathbb{E}\big[I_{\mathbf{s}}(n,d)\big] \\
&= \sum_{d \le 2n} \varphi(d) \left(1 - 2^{-\lfloor n(2,d)/d \rfloor}\right) \\
&= \sum_{d \in \mathcal{A}_{1,2}(n)} \varphi(d) \left(1 - 2^{-\lfloor n/d \rfloor}\right) + \sum_{d \in \mathcal{A}_{2,2}(2n)} \varphi(d) \left(1 - 2^{-\lfloor 2n/d \rfloor}\right) \\
&= \frac{3}{\pi^2} \left(c_{1,2} + 4c_{2,2}\right) \mathrm{Li}_2\big(\tfrac{1}{2}\big)\, n^2 + O\big(n(\log n)^2\big) \\
&= \frac{6}{\pi^2} \mathrm{Li}_2\big(\tfrac{1}{2}\big)\, n^2 + O\big(n(\log n)^2\big). \qquad (12)
\end{aligned}$$

Furthermore, from Lemma 6 and Lemma 7, we get that

$$\begin{aligned}
\mathbb{V}[X] &= \mathbb{E}\big[X^2\big] - \mathbb{E}[X]^2 \\
&= \sum_{d_1,\, d_2 \le 2n} \varphi(d_1)\, \varphi(d_2) \Big(\mathbb{E}\big[I_{\mathbf{s}}(n,d_1) I_{\mathbf{s}}(n,d_2)\big] - \mathbb{E}\big[I_{\mathbf{s}}(n,d_1)\big]\mathbb{E}\big[I_{\mathbf{s}}(n,d_2)\big]\Big) \\
&\le \sum_{[d_1,\, d_2] \le 2n} d_1 d_2\, 2^{-\lfloor n(2,d_1)/d_1 \rfloor - \lfloor n(2,d_2)/d_2 \rfloor + \lfloor n(2,[d_1,d_2])/[d_1,d_2] \rfloor} \left(1 - 2^{-\lfloor n(2,[d_1,d_2])/[d_1,d_2] \rfloor}\right) \\
&\le \sum_{[d_1,\, d_2] \le 2n} d_1 d_2 \left\lfloor \frac{n(2,[d_1,d_2])}{[d_1,d_2]} \right\rfloor \ll n \sum_{[d_1,\, d_2] \le 2n} (d_1, d_2) \ll n^3, \qquad (13)
\end{aligned}$$

where we also used the inequality $1 - 2^{-k} \le k/2$, which holds for every integer $k \ge 0$.

Therefore, by Chebyshev's inequality, (12), and (13), it follows that

$$\mathbb{P}\Big[\big|X - \mathbb{E}[X]\big| > \varepsilon\, \mathbb{E}[X]\Big] \le \frac{\mathbb{V}[X]}{\big(\varepsilon \mathbb{E}[X]\big)^2} \ll \frac{1}{\varepsilon^2 n} = o_\varepsilon(1),$$

as $n \to +\infty$. Hence, again by (12), we have

$$X \sim \mathbb{E}[X] \sim \frac{6}{\pi^2} \mathrm{Li}_2\big(\tfrac{1}{2}\big) n^2,$$

with probability $1 - o(1)$. Finally, thanks to Lemma 3, we have

$$\log \ell_{a,\mathbf{s}}(n) = X \log a + O_a\!\left(\frac{n^2}{\log n}\right),$$

and the asymptotic formula (4) follows. □

6 Acknowledgments

The author is grateful to the anonymous referee for providing many suggestions that improved the quality of the paper. The author is a member of GNSAGA of INdAM and of CrypTO, the group of Cryptography and Number Theory of Politecnico di Torino.

References

[1] S. Akiyama, Lehmer numbers and an asymptotic formula for π, *J. Number Theory* **36** (1990), 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), 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), 129–146.

[4] S. Akiyama and F. Luca, On the least common multiple of Lucas subsequences, *Acta Arith.* **161** (2013), 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), 4585–4603.

[6] J.-P. Bézivin, Plus petit commun multiple des termes consécutifs d'une suite récurrente linéaire, *Collect. Math.* **40** (1989), 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), 199–213.

[9] P. Kiss and F. Mátyás, An asymptotic formula for π, *J. Number Theory* **31** (1989), 255–259.

[10] Y. V. Matiyasevich and R. K. Guy, A new formula for π, *Amer. Math. Monthly* **93** (1986), 631–635.

[11] C. Sanna, Practical numbers in Lucas sequences, *Quaest. Math.* **42** (2019), 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 least common multiple of random q-integers, *Res. Number Theory* **7** (2021), 16.

[14] C. Sanna, On the l.c.m. of shifted Fibonacci numbers, *Int. J. Number Theory* (in press) https://doi.org/10.1142/S1793042121500743.

[15] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, 3rd edition, Vol. 163 of *Graduate Studies in Mathematics*, American Mathematical Society, 2015.

[16] B. Tropak, Some asymptotic properties of Lucas numbers, In *Proceedings of the Regional Mathematical Conference (Kalsk, 1988)*, pp. 49–55. Pedagog. Univ. Zielona Góra, 1990.

[17] D. Zagier, The dilogarithm function. In *Frontiers in Number Theory, Physics, and Geometry. II*, pp. 3–65. Springer, 2007.

2010 *Mathematics Subject Classification*: Primary 11B39; Secondary 11B37, 11N37.
Keywords: asymptotic formula, least common multiple, power.

Received March 24 2021; revised versions received May 22 2021; June 12 2021. Published June 12 2021.

Return to Journal of Integer Sequences home page.