



POLITECNICO DI TORINO  
Repository ISTITUZIONALE

On the l.c.m. of random terms of binary recurrence sequences

*Original*

On the l.c.m. of random terms of binary recurrence sequences / Sanna, C.. - In: JOURNAL OF NUMBER THEORY. - ISSN 0022-314X. - STAMPA. - 213(2020), pp. 221-231. [10.1016/j.jnt.2019.12.004]

*Availability:*

This version is available at: 11583/2818859 since: 2020-05-03T10:24:59Z

*Publisher:*

Academic Press Inc.

*Published*

DOI:10.1016/j.jnt.2019.12.004

*Terms of use:*

openAccess

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

*Publisher copyright*

Elsevier postprint/Author's Accepted Manuscript

© 2020. This manuscript version is made available under the CC-BY-NC-ND 4.0 license  
<http://creativecommons.org/licenses/by-nc-nd/4.0/>. The final authenticated version is available online at:  
<http://dx.doi.org/10.1016/j.jnt.2019.12.004>

(Article begins on next page)

# ON THE L.C.M. OF RANDOM TERMS OF BINARY RECURRENCE SEQUENCES

CARLO SANNA

ABSTRACT. For every positive integer  $n$  and every  $\delta \in [0, 1]$ , let  $B(n, \delta)$  denote the probabilistic model in which a random set  $A \subseteq \{1, \dots, n\}$  is constructed by choosing independently every element of  $\{1, \dots, n\}$  with probability  $\delta$ . Moreover, let  $(u_k)_{k \geq 0}$  be an integer sequence satisfying  $u_k = a_1 u_{k-1} + a_2 u_{k-2}$ , for every integer  $k \geq 2$ , where  $u_0 = 0$ ,  $u_1 \neq 0$ , and  $a_1, a_2$  are fixed nonzero integers; and let  $\alpha$  and  $\beta$ , with  $|\alpha| \geq |\beta|$ , be the two roots of the polynomial  $X^2 - a_1 X - a_2$ . Also, assume that  $\alpha/\beta$  is not a root of unity.

We prove that, as  $\delta n / \log n \rightarrow +\infty$ , for every  $A$  in  $B(n, \delta)$  we have

$$\log \text{lcm}(u_a : a \in A) \sim \frac{\delta \text{Li}_2(1 - \delta)}{1 - \delta} \cdot \frac{3 \log |\alpha / \sqrt{(a_1^2, a_2)}|}{\pi^2} \cdot n^2$$

with probability  $1 - o(1)$ , where  $\text{lcm}$  denotes the lowest common multiple,  $\text{Li}_2$  is the dilogarithm, and the factor involving  $\delta$  is meant to be equal to 1 when  $\delta = 1$ .

This extends previous results of Akiyama, Tropic, Matiyasevich, Guy, Kiss and Mátyás, who studied the deterministic case  $\delta = 1$ , and is motivated by an asymptotic formula for  $\text{lcm}(A)$  due to Cilleruelo, Rué, Šarka, and Zumalacárregui.

## 1. INTRODUCTION

It is well known that the Prime Number Theorem is equivalent to the asymptotic formula

$$(1) \quad \log \text{lcm}(1, 2, \dots, n) \sim n,$$

as  $n \rightarrow +\infty$ , where  $\text{lcm}$  denotes the lowest common multiple.

For every positive integer  $n$  and every  $\delta \in [0, 1]$ , let  $B(n, \delta)$  denote the probabilistic model in which a random set  $A \subseteq \{1, \dots, n\}$  is constructed by choosing independently every element of  $\{1, \dots, n\}$  with probability  $\delta$ . Motivated by (1), Cilleruelo, Rué, Šarka, and Zumalacárregui [8] proved the following result (see also [5] for a more precise version, and [6, 7, 12] for others results of similar flavor).

**Theorem 1.1.** *Let  $A$  be a random set in  $B(n, \delta)$ . Then, as  $\delta n \rightarrow +\infty$ , we have*

$$\log \text{lcm}(A) \sim \frac{\delta \log(1/\delta)}{1 - \delta} \cdot n,$$

with probability  $1 - o(1)$ , where the factor involving  $\delta$  is meant to be equal to 1 for  $\delta = 1$ .

Let  $(u_k)_{k \geq 0}$  be an integer sequence satisfying  $u_k = a_1 u_{k-1} + a_2 u_{k-2}$ , for every integer  $k \geq 2$ , where  $u_0 = 0$ ,  $u_1 \neq 0$ , and  $a_1, a_2$  are two fixed nonzero integers. Moreover, let  $\alpha$  and  $\beta$ , with  $|\alpha| \geq |\beta|$ , be the two roots of the polynomial  $X^2 - a_1 X - a_2$ . We assume that  $\alpha/\beta$  is not a root of unity, which is a necessary and sufficient condition to have  $u_k \neq 0$  for all integers  $k \geq 1$ .

Akiyama [1] and, independently, Tropic [15] proved the following analog of (1) for the sequence  $(u_k)_{k \geq 1}$ .

**Theorem 1.2.** *We have*

$$\log \text{lcm}(u_1, u_2, \dots, u_n) \sim \frac{3 \log |\alpha / \sqrt{(a_1^2, a_2)}|}{\pi^2} \cdot n^2,$$

---

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

*Key words and phrases.* binary recurrence sequence; lowest common multiple; Lehmer sequence; random sequence.

†C. Sanna is supported by a postdoctoral fellowship of INdAM and is a member of the INdAM group GNSAGA.

as  $n \rightarrow +\infty$ .

Special cases of Theorem 1.2 were previously proved by Matiyasevich, Guy [11], Kiss and Mátyás [10]. Furthermore, Akiyama [2, 3] generalized Theorem 1.2 to sequences having some special divisibility properties, while Akiyama and Luca [4] studied  $\text{lcm}(u_{f(1)}, \dots, u_{f(n)})$  when  $f$  is a polynomial,  $f = \varphi$  (the Euler's totient function),  $f = \sigma$  (the sum of divisors function), or  $f$  is a binary recurrence sequence.

Motivated by Theorem 1.1, we give the following generalization of Theorem 1.2.

**Theorem 1.3.** *Let  $A$  be a random set in  $B(n, \delta)$ . Then, as  $\delta n / \log n \rightarrow +\infty$ , we have*

$$(2) \quad \text{lcm}(u_a : a \in A) \sim \frac{\delta \text{Li}_2(1 - \delta)}{1 - \delta} \cdot \frac{3 \log |\alpha / \sqrt{(a_1^2, a_2)}|}{\pi^2} \cdot n^2,$$

with probability  $1 - o(1)$ , where  $\text{Li}_2(z) := \sum_{k=1}^{\infty} z^k / k^2$  is the dilogarithm and the factor involving  $\delta$  is meant to be equal to 1 when  $\delta = 1$ .

When  $\delta = 1/2$  all the subsets  $A \subseteq \{1, \dots, n\}$  are chosen by  $B(n, \delta)$  with the same probability. Hence, Theorem 1.3 together with the identity  $\text{Li}_2(\frac{1}{2}) = (\pi^2 - 6(\log 2)^2)/12$  (see, e.g., [16]) give the following result.

**Corollary 1.1.** *As  $n \rightarrow +\infty$ , we have*

$$\text{lcm}(u_a : a \in A) \sim \frac{1}{4} \left( 1 - \frac{6(\log 2)^2}{\pi^2} \right) \cdot \log \left| \frac{\alpha}{\sqrt{(a_1^2, a_2)}} \right| \cdot n^2,$$

uniformly for all sets  $A \subseteq \{1, \dots, n\}$ , but at most  $o(2^n)$  exceptions.

## 2. NOTATION

We employ the Landau–Bachmann “Big Oh” and “little oh” notations  $O$  and  $o$ , as well as the associated Vinogradov symbols  $\ll$  and  $\gg$ , with their usual meanings. Any dependence of the implied constants is explicitly stated or indicated with subscripts. For real random variables  $X$  and  $Y$ , we say that “ $X \sim Y$  with probability  $1 - o(1)$ ” if  $\mathbb{P}(|X - Y| \geq \varepsilon | Y|) = o_\varepsilon(1)$  for every  $\varepsilon > 0$ . We write  $\text{lcm}(S)$  for the lowest common multiple of the elements of  $S \subseteq \mathbb{Z}$ , with the convention  $\text{lcm}(\emptyset) := 1$ . We also let  $[a, b]$  and  $(a, b)$  denote the lowest common multiple and the greatest common divisor, respectively, of two integers  $a$  and  $b$ . Throughout, the letters  $p$  is reserved for prime numbers, and  $\nu_p$  denotes the  $p$ -adic valuation. As usual, we write  $\Lambda(n)$ ,  $\varphi(n)$ ,  $\tau(n)$ , and  $\mu(n)$ , for the von Mangoldt function, the Euler's totient function, the number of divisors, and the Möbius function of a positive integer  $n$ , respectively.

## 3. PRELIMINARIES ON LEHMER SEQUENCES

Let  $\zeta$  and  $\eta$  be complex numbers such that  $c_1 := (\zeta + \eta)^2$  and  $c_2 := \zeta\eta$  are nonzero coprime integers and  $\zeta/\eta$  is not a root of unity. Also, assume  $|\zeta| \geq |\eta|$ . The *Lehmer sequence*  $(\tilde{u}_k)_{k \geq 0}$  associated to  $\zeta$  and  $\eta$  is defined by

$$(3) \quad \tilde{u}_k := \begin{cases} (\zeta^k - \eta^k) / (\zeta - \eta) & \text{if } k \text{ is odd,} \\ (\zeta^k - \eta^k) / (\zeta^2 - \eta^2) & \text{if } k \text{ is even,} \end{cases}$$

for every integer  $k \geq 0$ . It is known that  $(\tilde{u}_k)_{k \geq 1}$  is an integer sequence. For every positive integer  $m$  coprime with  $c_2$ , let  $\varrho(m)$  be the *rank of appearance* of  $m$  in the Lehmer sequence  $(\tilde{u}_k)_{k \geq 0}$ , that is, the smallest positive integer  $k$  such that  $m \mid \tilde{u}_k$ . It is known that  $\varrho(m)$  exists. Moreover, for every prime number  $p$  not dividing  $c_2$ , put  $\kappa(p) := \nu_p(\tilde{u}_{\varrho(p)})$ .

We need the following properties of the rank of appearance.

**Lemma 3.1.** *We have:*

- (i)  $m \mid \tilde{u}_k$  if and only if  $(m, c_2) = 1$  and  $\varrho(m) \mid k$ , for all integers  $m, k \geq 1$ .
- (ii)  $\varrho(p^k) = p^{\max(k - \kappa(p), 0)} \varrho(p)$ , for all primes  $p$  not dividing  $2c_2$  and all integers  $k \geq 1$ .

(iii)  $\varrho(2^k) = 2^{\max(k - \nu_2(\tilde{u}_{\varrho(4)}), 0)} \varrho(4)$ , for all integers  $k \geq 2$ .

*Proof.* (i) We have  $(\tilde{u}_k, c_2) = 1$  for all integers  $k \geq 1$  [13, Lemma 1]. Also,  $(\tilde{u}_k, \tilde{u}_h) = \tilde{u}_{(k,h)}$  for all integers  $k, h \geq 1$  [13, Lemma 3]. Hence, on the one hand, if  $m \mid \tilde{u}_k$  then  $(m, c_2) = 1$  and  $m \mid (\tilde{u}_k, \tilde{u}_{\varrho(m)}) = \tilde{u}_{(k, \varrho(m))}$ , which in turn implies that  $\varrho(m) \mid k$ , by the minimality of  $\varrho(m)$ . On the other hand, if  $(c_2, m) = 1$  and  $\varrho(m) \mid k$  then  $m \mid \tilde{u}_{\varrho(m)} = \tilde{u}_{(k, \varrho(m))} = (\tilde{u}_k, \tilde{u}_{\varrho(m)})$ , so that  $m \mid \tilde{u}_k$ .

(ii) If  $p \mid \tilde{u}_m$ , for some positive integer  $m$ , then  $p \parallel \tilde{u}_{pm}/\tilde{u}_m$  [13, Lemma 5]. Hence, it follows by induction on  $h$  that  $\nu_p(\tilde{u}_{p^h \varrho(p)}) = \kappa(p) + h$ , for every integer  $h \geq 0$ . At this point, the claim follows easily from (i).

(iii) If  $4 \mid \tilde{u}_m$ , for some positive integer  $m$ , then  $2 \parallel \tilde{u}_{pm}/\tilde{u}_m$  [13, Lemma 5]. The proof proceeds similarly to the previous point.  $\square$

Hereafter, in light of Lemma 3.1(i), in subscripts of sums and products the argument of  $\varrho$  is always tacitly assumed to be coprime with  $c_2$ .

Let us define the cyclotomic numbers  $(\phi_k)_{k \geq 1}$  associated to  $\zeta$  and  $\eta$  by

$$(4) \quad \phi_k := \prod_{\substack{1 \leq h \leq k \\ (h, k) = 1}} \left( \zeta - e^{\frac{2\pi i h}{k}} \eta \right),$$

for every integer  $k \geq 0$ . It can be proved that  $\phi_k \in \mathbb{Z}$  for every integer  $k \geq 3$ . Moreover, from (4) it follows easily that

$$\zeta^k - \eta^k = \prod_{d \mid k} \phi_d,$$

which in turn, applying Möbius inversion formula and taking into account (3), gives

$$(5) \quad \phi_k = \prod_{d \mid k} \left( \zeta^d - \eta^d \right)^{\mu(k/d)} = \prod_{d \mid k} \tilde{u}_d^{\mu(k/d)},$$

for all integers  $k \geq 3$ . We need the following result about  $\phi_k$ .

**Lemma 3.2.** *For every integer  $k \geq 13$ , we have*

$$|\phi_k| = \lambda_k \cdot \prod_{\varrho(p) = k} p^{\kappa(p)},$$

where  $\lambda_k$  is equal to 1 or to the greatest prime factor of  $k/(k, 3)$ .

*Proof.* Let  $p$  be a prime number not dividing  $c_2$ . By the definition of  $\varrho(p)$ , we have that  $p \nmid \tilde{u}_h$  for each positive integer  $h < \varrho(p)$ . Hence, by (5), we obtain that  $\nu_p(\phi_{\varrho(p)}) = \nu_p(\tilde{u}_{\varrho(p)}) = \kappa(p)$ . In particular,  $p \mid \phi_{\varrho(p)}$ . Let  $k \geq 3$  be an integer and suppose that  $p$  is a prime factor of  $\phi_k$ . On the one hand, if  $\varrho(p) = k$  then, by the previous consideration,  $\nu_p(\phi_k) = \kappa(p)$ . On the other hand, if  $\varrho(p) \neq k$  then  $p \mid (\phi_{\varrho(p)}, \phi_k)$ . Finally, for  $k \geq 13$  and for every integer  $h \geq 3$  with  $h \neq k$ , we have that  $(\phi_h, \phi_k)$  divides the greatest prime factor of  $k/(k, 3)$  [13, Lemma 7].  $\square$

We conclude this section with a formula for a sum involving the von Mangoldt function.

**Lemma 3.3.** *We have*

$$(6) \quad \sum_{\varrho(m) = r} \Lambda(m) = \varphi(r) \log |\zeta| + O_{\zeta, \eta}(\tau(r) \log(r + 1)),$$

and, in particular,

$$(7) \quad \sum_{\varrho(m) = r} \Lambda(m) \ll_{\zeta, \eta} \varphi(r),$$

for every positive integer  $r$ .

*Proof.* Clearly, we can assume  $r \geq 13$ . Write  $m = p^k$ , where  $p$  is a prime number not dividing  $c_2$  and  $k$  is a positive integer. First, suppose that  $p > 2$ . By Lemma 3.1(ii), we have that  $\varrho(m) = p^{\max(k-\kappa(p),0)} \varrho(p)$ . Hence,  $\varrho(m) = r$  if and only if  $k \leq \kappa(p)$  and  $\varrho(p) = r$ , or  $k > \kappa(p)$  and  $p^{k-\kappa(p)} \varrho(p) = r$ . In the first case, the contribution to the sum in (6) is exactly  $\kappa(p) \log p$ . In the second case,  $p \mid r$  and, since  $k$  is determined by  $p$  and  $r$ , the contribution to the sum in (6) is  $\log p$ . Using Lemma 3.1(iii), the case  $p = 2$  can be handled similarly. Therefore,

$$(8) \quad \sum_{\varrho(m)=r} \Lambda(m) = \sum_{\varrho(p)=r} \kappa(p) \log p + O\left(\sum_{p \mid r} \log p\right) = \log |\phi_r| + O(\log r),$$

where we used Lemma 3.2. Furthermore, from (5) and the identity  $\sum_{d \mid r} \mu(r/d) d = \varphi(r)$ , it follows that

$$\log |\phi_r| = \varphi(r) \log |\zeta| + O\left(\sum_{d \mid r} \log \left|1 - \left(\frac{\eta}{\zeta}\right)^d\right|\right).$$

If  $|\eta/\zeta| < 1$  then  $\log |1 - (\eta/\zeta)^d| = O_{\zeta,\eta}(1)$ . If  $|\eta/\zeta| = 1$  then, since  $\eta/\zeta$  is an algebraic number that is not a root of unity, it follows from classic bounds on linear forms in logarithms (see, e.g., [9, Lemma 3]) that  $\log |1 - (\eta/\zeta)^d| = O_{\zeta,\eta}(\log(d+1))$ . Consequently,

$$(9) \quad \log |\phi_r| = \varphi(r) \log |\zeta| + O_{\zeta,\eta}(\tau(r) \log(r+1)).$$

Putting together (8) and (9), we get (6). Finally, the upper bound (7) follows since  $\tau(k) \leq k^\varepsilon$  and  $\varphi(k) \geq k^{1-\varepsilon}$ , for all  $\varepsilon > 0$  and every integer  $k \gg_\varepsilon 1$  [14, Ch. I.5, Corollary 1.1 and Eq. 12].  $\square$

#### 4. FURTHER PRELIMINARIES

We need two estimates involving the Euler's totient function. Define

$$\Phi(x) := \sum_{n \leq x} \varphi(n),$$

for every  $x \geq 1$ .

**Lemma 4.1.** *We have*

$$\Phi(x) = \frac{3}{\pi^2} x^2 + O(x \log x) \quad \text{and} \quad \sum_{n \leq x} \frac{\varphi(n)}{n} \ll x,$$

for every  $x \geq 2$ .

*Proof.* The first formula is well known [14, Ch. I.3, Thm. 4] and implies

$$\sum_{n \leq x} \frac{\varphi(n)}{n} \leq \sum_{n \leq x/2} 1 + \sum_{x/2 < n \leq x} \frac{\varphi(n)}{x/2} \ll x,$$

as desired.  $\square$

The following lemma is an easy inequality that will be useful later.

**Lemma 4.2.** *It holds  $1 - (1-x)^k \leq kx$ , for all  $x \in [0, 1]$  and all integers  $k \geq 0$ .*

*Proof.* The claim is  $(1 + (-x))^k \geq 1 + k(-x)$ , which follows from Bernoulli's inequality.  $\square$

## 5. PROOF OF THEOREM 1.3

Henceforth, all the implied constants may depend by  $a_1$ ,  $a_2$ , and  $u_1$ . It is well known that the generalized Binet's formula

$$(10) \quad u_k = \frac{\alpha^k - \beta^k}{\alpha - \beta} u_1,$$

holds for every integer  $k \geq 0$ . We put  $\zeta := \alpha/\sqrt{b}$  and  $\eta := \beta/\sqrt{b}$ , where  $b := (a_1^2, a_2)$ . Note that indeed  $c_1 = a_1^2/b$  and  $c_2 = -a_2/b$  are nonzero relatively prime integers,  $\zeta/\eta = \alpha/\beta$  is not a root of unity, and  $|\zeta| \geq |\eta|$ . Moreover, from (3) and (10), it follows easily that

$$u_k = \begin{cases} b^{(k-1)/2} u_1 \tilde{u}_k & \text{if } k \text{ is odd,} \\ a_1 b^{k/2-1} u_1 \tilde{u}_k & \text{if } k \text{ is even,} \end{cases}$$

for every integer  $k \geq 0$ . Therefore, for every  $A \subseteq \{1, \dots, n\}$ , we have

$$\log \text{lcm}(u_a : a \in A) = \log \text{lcm}(\tilde{u}_a : a \in A) + O(n).$$

Note that  $O(n)$  is a ‘‘little oh’’ of the right-hand side of (2), as  $\delta n / \log n \rightarrow +\infty$ . Hence, it is enough to prove Theorem 1.3 with  $\log \text{lcm}(\tilde{u}_a : a \in A)$  in place of  $\log \text{lcm}(u_a : a \in A)$ , and this will be indeed our strategy.

Hereafter, let  $A$  be a random set in  $B(n, \delta)$ , and put  $L := \text{lcm}(\tilde{u}_a : a \in A)$  and  $X := \log L$ . For every positive integer  $m$  coprime with  $c_2$ , let us define

$$I_A(m) := \begin{cases} 1 & \text{if } \varrho(m) \mid a \text{ for some } a \in A, \\ 0 & \text{otherwise.} \end{cases}$$

The following lemma gives an expression for  $X$  in terms of  $I_A$  and the von Mangoldt function.

**Lemma 5.1.** *We have*

$$X = \sum_{\varrho(m) \leq n} \Lambda(m) I_A(m).$$

*Proof.* For every prime power  $p^k$  with  $p \nmid c_2$ , we know from Lemma 3.1(i) that  $p^k \mid L$  if and only if  $\varrho(p^k) \mid a$  for some  $a \in A$  and, in particular,  $\varrho(p^k) \leq n$ . Hence,

$$X = \sum_{p^k \mid L} \log p = \sum_{\varrho(p^k) \leq n} (\log p) I_A(p^k) = \sum_{\varrho(m) \leq n} \Lambda(m) I_A(m),$$

as claimed.  $\square$

The next lemma provides two expected values involving  $I_A$  and needed in later arguments.

**Lemma 5.2.** *We have*

$$(11) \quad \mathbb{E}(I_A(m)) = 1 - (1 - \delta)^{\lfloor n/\varrho(m) \rfloor}$$

and

$$\begin{aligned} \mathbb{E}(I_A(m)I_A(\ell)) &= 1 - (1 - \delta)^{\lfloor n/\varrho(m) \rfloor} - (1 - \delta)^{\lfloor n/\varrho(\ell) \rfloor} \\ &\quad + (1 - \delta)^{\lfloor n/\varrho(m) \rfloor + \lfloor n/\varrho(\ell) \rfloor - \lfloor n/[\varrho(m), \varrho(\ell)] \rfloor}, \end{aligned}$$

for all positive integers  $m$  and  $\ell$  with  $(m\ell, c_2) = 1$ .

*Proof.* By the definition of  $I_A$ , we have

$$\mathbb{E}(I_A(m)) = \mathbb{P}(\exists a \in A : \varrho(m) \mid a) = 1 - \mathbb{P}\left(\bigwedge_{t \leq n/\varrho(m)} (\varrho(m)t \notin A)\right) = 1 - (1 - \delta)^{\lfloor n/\varrho(m) \rfloor},$$

which is the first claim. On the one hand, by linearity of expectation and by (11), we obtain

$$\begin{aligned} \mathbb{E}(I_A(m)I_A(\ell)) &= \mathbb{E}(I_A(m) + I_A(\ell) - 1 + (1 - I_A(m))(1 - I_A(\ell))) \\ &= \mathbb{E}(I_A(m)) + \mathbb{E}(I_A(\ell)) - 1 + \mathbb{E}((1 - I_A(m))(1 - I_A(\ell))) \end{aligned}$$

$$= 1 - (1 - \delta)^{\lfloor n/\varrho(m) \rfloor} - (1 - \delta)^{\lfloor n/\varrho(\ell) \rfloor} + \mathbb{E}((1 - I_A(m))(1 - I_A(\ell))).$$

On the other hand, by the definition of  $I_A$ ,

$$\begin{aligned} \mathbb{E}((1 - I_A(m))(1 - I_A(\ell))) &= \mathbb{P}(\forall a \in A : \varrho(m) \nmid a \text{ and } \varrho(\ell) \nmid a) \\ &= \mathbb{P}\left(\bigwedge_{\substack{k \leq n \\ \varrho(m) \mid k \text{ or } \varrho(\ell) \mid k}} (k \notin A)\right) = (1 - \delta)^{\lfloor n/\varrho(m) \rfloor + \lfloor n/\varrho(\ell) \rfloor - \lfloor n/[\varrho(m), \varrho(\ell)] \rfloor}, \end{aligned}$$

and the second claim follows too.  $\square$

Now we give an asymptotic formula for the expected value of  $X$ .

**Lemma 5.3.** *We have*

$$\mathbb{E}(X) = \frac{\delta \operatorname{Li}_2(1 - \delta)}{1 - \delta} \cdot \frac{3 \log |\zeta|}{\pi^2} \cdot n^2 + O(\delta n (\log n)^3),$$

for all integers  $n \geq 2$ . In particular,

$$\mathbb{E}(X) \sim \frac{\delta \operatorname{Li}_2(1 - \delta)}{1 - \delta} \cdot \frac{3 \log |\zeta|}{\pi^2} \cdot n^2,$$

as  $n \rightarrow +\infty$ , uniformly for  $\delta \in (0, 1]$ .

*Proof.* From Lemma 5.1 and Lemma 5.2, it follows that

$$\begin{aligned} \mathbb{E}(X) &= \sum_{\varrho(m) \leq n} \Lambda(m) \mathbb{E}(I_A(m)) \\ &= \sum_{\varrho(m) \leq n} \Lambda(m) (1 - (1 - \delta)^{\lfloor n/\varrho(m) \rfloor}) \\ &= \sum_{r \leq n} (1 - (1 - \delta)^{\lfloor n/r \rfloor}) \sum_{\varrho(m) = r} \Lambda(m). \end{aligned}$$

Consequently, thanks to Lemma 3.3 and Lemma 4.2, we obtain

$$\begin{aligned} (12) \quad \mathbb{E}(X) &= \sum_{r \leq n} (1 - (1 - \delta)^{\lfloor n/r \rfloor}) \varphi(r) \log |\zeta| + O\left(\delta n \sum_{r \leq n} \frac{\tau(r) \log(r+1)}{r}\right) \\ &= \sum_{r \leq n} (1 - (1 - \delta)^{\lfloor n/r \rfloor}) \varphi(r) \log |\zeta| + O(\delta n (\log n)^3), \end{aligned}$$

where we used the fact that

$$\sum_{r \leq n} \frac{\tau(r)}{r} \leq \left(\sum_{s \leq n} \frac{1}{s}\right)^2 \ll (\log n)^2.$$

Note that  $\lfloor n/r \rfloor = j$  if and only if  $r \in (n/(j+1), n/j]$ . Hence,

$$\begin{aligned} (13) \quad \sum_{r \leq n} (1 - (1 - \delta)^{\lfloor n/r \rfloor}) \varphi(r) &= \sum_{j \leq n} (1 - (1 - \delta)^j) \sum_{n/(j+1) < r \leq n/j} \varphi(r) \\ &= \sum_{j \leq n} (1 - (1 - \delta)^j) \left(\Phi\left(\frac{n}{j}\right) - \Phi\left(\frac{n}{j+1}\right)\right) \\ &= \delta \sum_{j \leq n} (1 - \delta)^{j-1} \Phi\left(\frac{n}{j}\right) \\ &= \delta \sum_{j \leq n} \frac{(1 - \delta)^{j-1}}{j^2} \cdot \frac{3}{\pi^2} \cdot n^2 + O\left(\delta \sum_{j \leq n} \frac{n}{j} \log\left(\frac{n}{j}\right)\right) \end{aligned}$$

$$= \frac{\delta \operatorname{Li}_2(1 - \delta)}{1 - \delta} \cdot \frac{3}{\pi^2} \cdot n^2 + O(\delta n (\log n)^2),$$

where we used Lemma 4.1. Finally, putting together (12) and (13), we get the desired claim.  $\square$

The next lemma is an upper bound for the variance of  $X$ .

**Lemma 5.4.** *We have*

$$\mathbb{V}(X) \ll \delta n^3 \log n,$$

for all integers  $n \geq 2$ .

*Proof.* On the one hand, by Lemma 5.1, we have

$$\begin{aligned} \mathbb{V}(X) &= \mathbb{E}(X^2) - \mathbb{E}(X)^2 \\ &= \sum_{\varrho(m), \varrho(\ell) \leq n} \Lambda(m) \Lambda(\ell) (\mathbb{E}(I_A(m) I_A(\ell)) - \mathbb{E}(I_A(m)) \mathbb{E}(I_A(\ell))). \end{aligned}$$

On the other hand, from Lemma 5.2 and Lemma 4.2, it follows that

$$\begin{aligned} &\mathbb{E}(I_A(m) I_A(\ell)) - \mathbb{E}(I_A(m)) \mathbb{E}(I_A(\ell)) \\ &= (1 - \delta)^{\lfloor n/\varrho(m) \rfloor + \lfloor n/\varrho(\ell) \rfloor - \lfloor n/[\varrho(m), \varrho(\ell)] \rfloor} (1 - (1 - \delta)^{\lfloor n/[\varrho(m), \varrho(\ell)] \rfloor}) \leq \frac{\delta n}{[\varrho(m), \varrho(\ell)]}. \end{aligned}$$

Therefore,

$$\begin{aligned} (14) \quad \mathbb{V}(X) &\leq \delta n \sum_{\varrho(m), \varrho(\ell) \leq n} \frac{\Lambda(m) \Lambda(\ell)}{[\varrho(m), \varrho(\ell)]} = \delta n \sum_{r, s \leq n} \frac{1}{[r, s]} \sum_{\varrho(m)=r} \Lambda(m) \sum_{\varrho(\ell)=s} \Lambda(\ell) \\ &\ll \delta n \sum_{r, s \leq n} \frac{\varphi(r) \varphi(s)}{[r, s]} = \delta n \sum_{r, s \leq n} (r, s) \frac{\varphi(r) \varphi(s)}{rs}, \end{aligned}$$

where we used Lemma 3.3 and the identity  $[r, s] = rs/(r, s)$ . At this point, writing  $r = dr'$  and  $s = ds'$ , where  $d := (r, s)$ , we obtain

$$\begin{aligned} (15) \quad \sum_{r, s \leq n} (r, s) \frac{\varphi(r) \varphi(s)}{rs} &= \sum_{d \leq n} d \sum_{\substack{r', s' \leq n/d \\ (r', s')=1}} \frac{\varphi(dr') \varphi(ds')}{d^2 r' s'} \leq \sum_{d \leq n} d \left( \sum_{t \leq n/d} \frac{\varphi(t)}{t} \right)^2 \\ &\ll \sum_{d \leq n} d \left( \frac{n}{d} \right)^2 \ll n^2 \log n, \end{aligned}$$

where we used Lemma 4.1 and the inequality  $\varphi(dm) \leq d\varphi(m)$ , holding for every integer  $m \geq 1$ . Finally, putting together (14) and (15), we get the desired claim.  $\square$

*Proof of Theorem 1.3.* By Chebyshev's inequality, Lemma 5.3, and Lemma 5.4, we have

$$\mathbb{P}(|X - \mathbb{E}(X)| \geq \varepsilon \mathbb{E}(X)) \leq \frac{\mathbb{V}(X)}{(\varepsilon \mathbb{E}(X))^2} \ll \frac{\log n}{\varepsilon^2 \delta n} = o_\varepsilon(1),$$

as  $\delta n / \log n \rightarrow +\infty$ . Hence, again by Lemma 5.3, we have

$$X \sim \frac{\delta \operatorname{Li}_2(1 - \delta)}{1 - \delta} \cdot \frac{3 \log |\zeta|}{\pi^2} \cdot n^2,$$

with probability  $1 - o(1)$ , as desired.  $\square$



## REFERENCES

1. S. Akiyama, *Lehmer numbers and an asymptotic formula for  $\pi$* , 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., Published electronically: July 2, 2019.
6. J. Cilleruelo and J. Guíjarro-Ordóñez, *Ratio sets of random sets*, Ramanujan J. **43** (2017), no. 2, 327–345.
7. J. Cilleruelo, D. S. Ramana, and O. Ramaré, *Quotient and product sets of thin subsets of the positive integers*, Proc. Steklov Inst. Math. **296** (2017), no. 1, 52–64.
8. 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.
9. P. Kiss, *Primitive divisors of Lucas numbers*, Applications of Fibonacci numbers (San Jose, CA, 1986), Kluwer Acad. Publ., Dordrecht, 1988, pp. 29–38.
10. P. Kiss and F. Mátyás, *An asymptotic formula for  $\pi$* , J. Number Theory **31** (1989), no. 3, 255–259.
11. Y. V. Matiyasevich and R. K. Guy, *A new formula for  $\pi$* , Amer. Math. Monthly **93** (1986), no. 8, 631–635.
12. C. Sanna, *A note on product sets of random sets*, Acta Math. Hungar. (accepted)
13. C. L. Stewart, *On divisors of Fermat, Fibonacci, Lucas, and Lehmer numbers*, Proc. London Math. Soc. (3) **35** (1977), no. 3, 425–447.
14. G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics, vol. 46, Cambridge University Press, Cambridge, 1995.
15. 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.
16. D. Zagier, *The dilogarithm function*, Frontiers in number theory, physics, and geometry. II, Springer, Berlin, 2007, pp. 3–65.

UNIVERSITÀ DI GENOVA, DEPARTMENT OF MATHEMATICS, GENOVA, ITALY  
 Email address: carlo.sanna.dev@gmail.com