On the least common multiple of Lucas subsequences

Shigeki Akiyama
Institute of Mathematics
University of Tsukuba
Tennodai 1-1-1, Tsukuba, Ibaraki
305-8571, Japan
akiyama@math.tsukuba.ac.jp

Florian Luca
Fundación Marcos Moshinsky, UNAM
Circuito Exterior, C.U., Apdo. Postal 70-543
Mexico D.F. 04510, Mexico
fluca@matmor.unam.mx

Abstract

We compare growth of the least common multiple of the numbers $u_{a_1}, u_{a_2}, \ldots, u_{a_n}$ and $|u_{a_1}u_{a_2}\cdots u_{a_n}|$, where $(u_n)_{n\geq 0}$ is a Lucas sequence and $(a_n)_{n\geq 0}$ is some sequence of positive integers.

2000 Mathematics Subject Classification: 11A05, 11B39

Keywords: Primitive divisor, Least common multiple, Lucas-Lehmer sequence

1 Introduction

Matiyazevich and Guy [15] proved the interesting formula:

$$\lim_{n\to\infty} \frac{\log F_1 \cdots F_n}{\log \operatorname{lcm}(F_1, \ldots, F_n)} = \frac{\pi^2}{6}$$

valid for the Fibonacci numbers defined by $F_0 = 0, F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 0$. Since the least common multiple grows by the contributions of the powers of the *primitive prime divisors*, that is, the prime factors appearing in F_n but not in F_m for any $m < n$, the point of the proof is to describe effectively the contribution of the powers of the primitive prime divisors. Inspired by this formula, several generalizations are discussed in [1, 2, 3, 13] for other sequences of integers $(b_n)_{n\geq 0}$. A clue of these results is the *strong divisibility* condition:

$$\text{(S)} \qquad (b_n, b_m) = |b_{\gcd(m,n)}|.$$

The above property assures that the primitive divisors of b_n are essentially given by the inclusion-exclusion formula

$$\prod_{d|n} b_{n/d}^{\mu(d)},$$

and allows us to control the growth of the least common multiple. This is why, strong divisibility and primitive divisors attracted the attention of many researchers [4, 6, 9, 14, 17]. Especially, a lot of effort was spent on the primitive divisors of elliptic divisibility sequences [8, 10, 11, 22].

There are few known results of the above type for general sequences without the assumption (S). In this paper, we give several results on subsequences of Lucas-Lehmer sequences, or *Lucas subsequences* for short, which do not satisfy (S). Let $(u_n)_{n\geq 0}$ is the non-degenerate binary linear sequence given by the recurrence $u_{n+2} = Au_{n+1} + Bu_n$ for all $n \geq 0$, where $u_0 = 0,\ u_1 \neq 0$, A and B are fixed non–zero integers. By non-degenerate we mean that the equation $x^2 - Ax - B = 0$ has two nonzero roots $\alpha,\ \beta$ such that α/β is not a root of 1. In this case, the Binet formula

$$u_n = u_1 \left(\frac{\alpha^n - \beta^n}{\alpha - \beta} \right) \quad \text{holds for all} \quad n \geq 0. \tag{1}$$

We assume that $|\alpha| \geq |\beta|$ and put $\kappa = \log \gcd(A^2, B)/2 \log |\alpha|$. We compute several cases of $(a_n)_{n\geq 0}$. We adopt the convention that $\operatorname{lcm}[s \in \mathcal{S}]$ means the least common multiple of the *nonzero* elements s of $\mathcal{S}$.

Theorem 1. *If $a_n = |f(n)|$ for all $n \geq 1$, where $f(X) \in \mathbb{Z}[X]$ has at least two distinct roots, then*

$$\frac{\log \left| \prod_{\substack{1\leq k\leq n \\ a_k \neq 0}} u_{a_k} \right|}{\log \operatorname{lcm}[u_{a_1}, \ldots, u_{a_n}]} = \frac{1}{1-\kappa} + O\left(\frac{1}{\log n} \right). \tag{2}$$

Theorem 2. *When* $f(X) = C(aX+b)^m \in \mathbb{Z}[X]$ *with* $a > 0$ *and* b *coprime, then*

$$\frac{\log \left|\prod_{\substack{1\le k\le n\\ a_k\neq 0}} u_{a_k}\right|}{\log \operatorname{lcm}[u_{a_1},\ldots,u_{a_n}]} = \frac{\zeta(m+1)}{1-\kappa}\prod_{p\mid a}\left(1-\frac{1}{p^{m+1}}\right) + O\left(\frac{1}{\log n}\right).$$

We also treat the cases in which $(a_n)_{n\ge 0}$ is some arithmetic function of n, such as the Euler function $\phi(n)$ and the sum of divisors function $\sigma(n)$ (see Theorem 3, as well as the case when $(a_n)_{n\ge 0}$ is a non–degenerate binary recurrent sequence (see Theorem 4).

Note that when $b = 0$, u_{a_n} satisfies (S) and we recover the main term of [2]. The error term becomes worse because of the generality of our method. The factor $1/(1-\kappa)$ simply comes from the common divisor of all u_{a_n} and is not so important. The main terms of the two theorems give a sharp contrast. We observe some dichotomy: whenever there are distinct factors the least common multiple and the product of subsequences become essentially the same.

Throughout the paper, we use the Landau symbols O and o and the Vinogradov symbols $\gg$, $\ll$ with their usual meaning. We recall that $A = O(B)$, $A \ll B$ and $B \gg A$ are all equivalent and mean that $|A| \le cB$ holds with some positive constant c, while $A = o(B)$ means that $A/B \to 0$. We also use $c_1,\ c_2,\ \ldots$ for positive computable constants. All constants which appear depend on our sequences $(u_n)_{n\ge 0}$ and $(a_n)_{n\ge 0}$.

2 Generalities

Clearly, $|\alpha| > 1$. By Baker's method, we have

$$|u_m| = |\alpha|^m |u_1||\alpha-\beta|^{-1}|1-(\beta/\alpha)^m| = \exp(m\log|\alpha| + O(\log(m+1))).$$

Evaluating this relation in $m = a_k$ for $k = 1,\ldots,n$, taking logarithms and summing we get

$$\log|u_{a_1}\cdots u_{a_n}| = \log|\alpha|\sum_{k=1}^n a_k + O\left(\sum_{k=1}^n \log(a_k+1)\right). \tag{3}$$

So, in applications, we shall need some information about

$$A_1(n) = \sum_{k=1}^n a_k \qquad \text{and} \qquad E_1(n) = \sum_{k=1}^n \log(a_k+1). \tag{4}$$

To deal with the least common multiple, we start as many authors do, by putting $T = \gcd(A^2, B)$, $v_n = T^{-n/2} u_n$, $A_1 = A/\sqrt{T}$, and $B_1 = B/T$. Then

$$v_n = \frac{u_1}{\sqrt{T}} \frac{\alpha_1^n - \beta_1^n}{\alpha_1 - \beta_1},$$

where $\alpha_1 = \alpha/\sqrt{T}$, $\beta_1 = \beta/\sqrt{T}$. Here, A_1^2 and B_1 are coprime integers and α_1, β_1 are the two roots of the equation $x^2 - A_1^2 x - B_1 = 0$. Put

$$w_n = \begin{cases} \frac{\alpha_1^n - \beta_1^n}{\alpha_1 - \beta_1} & \text{if} \quad n \equiv 1 \pmod 2, \\ \frac{\alpha_1^n - \beta_1^n}{\alpha_1^2 - \beta_1^2} & \text{if} \quad n \equiv 0 \pmod 2, \end{cases} \tag{5}$$

for the Lehmer numbers of roots α_1, β_1. Then

$$u_n = \begin{cases} u_1 T^{(n-1)/2} w_n & \text{if} \quad n \equiv 1 \pmod 2, \\ A u_1 T^{n/2-1} w_n & \text{if} \quad n \equiv 0 \pmod 2. \end{cases} \tag{6}$$

Let $\mathcal{S}$ be the set of all primes dividing ATu_1 and for a prime p and a nonzero integer m let $\mu_p(m)$ be the exponent with which p appears in the factorization of m. Since A_1^2 and B_1 are coprime, from linear forms in p-adic logarithms, we have $\mu_p(w_n) < c_p \log n$, where c_p is some constant depending on p. We put

$$\operatorname{lcm}[u_{a_1}, u_{a_2}, \ldots, u_{a_n}] =: M_1 M_2, \tag{7}$$

where M_1 is the contribution to the above least common multiple of the primes from $\mathcal{S}$ and M_2 is the remaining cofactor. The above comments show that

$$\begin{aligned} \log M_1 &= \left(\frac{\log T}{2}\right) \max\{a_k\}_{1 \le k \le n} + O\left(E_1(n)\right), \\ \log M_2 &= \log \operatorname{lcm}[w_{a_1}, \ldots, w_{a_n}] + O\left(E_1(n)\right). \end{aligned} \tag{8}$$

Next, we use cyclotomy to write

$$w_n = \prod_{d|n} \Phi_d(\alpha_1, \beta_1), \tag{9}$$

where we put

$$\Phi_m(\alpha_1, \beta_1) = \prod_{\substack{1 \le k \le m \\ \gcd(k,m)=1}} (\alpha_1 - e^{2\pi i k/m} \beta_1) \quad \text{for all} \quad m \ge 3, \tag{10}$$

and $\Phi_1(\alpha_1,\beta_1) = \Phi_2(\alpha_1,\beta_1) = 1$. It is well–known that $\Phi_m(\alpha_1,\beta_1)$ is an integer which captures the primitive prime factors of the term w_m. More precisely, if we put $\Psi_m(\alpha_1,\beta_1)$ to be the largest divisor of $\Phi_m(\alpha_1,\beta_1)$ consisting of primes which do not divide $\Phi_\ell(\alpha_1,\beta_1)$ for any $1 \le \ell \le m$, then

$$\Phi_m(\alpha_1,\beta_1) = \delta_m \Psi_m(\alpha_1,\beta_1), \tag{11}$$

where δ_m is a divisor of m (see [19], Lemmas 6,7,8). By Baker's method again, we have

$$\begin{aligned} |\Phi_m(\alpha_1,\beta_1)| &= \prod_{d|m} |\alpha_1^d - \beta_1^d|^{\mu(m/d)} \\ &= \prod_{d|m} |\alpha_1|^{d\mu(m/d)} |1-(\beta_1/\alpha_1)^d|^{\mu(m/d)} \\ &= \exp\left(\log|\alpha_1|\phi(m) + O(\tau(m)\log(m+1))\right). \end{aligned} \tag{12}$$

We evaluate the above relation at $m = a_k$ for $k = 1,\ldots,n$ and use the fact that

$$\log \prod_{k=1}^n \delta_{a_k} = O\left(\sum_{k=1}^n \log(a_k+1)\right) = O(E_1(n)), \tag{13}$$

to conclude that if we put

$$\mathcal{D}_n = \{d : d \mid a_k \text{ for some } 1 \le k \le n\}, \tag{14}$$

then from (9), (10), (11), (12) and (13) we obtain

$$\begin{aligned} \log \operatorname{lcm}[w_{a_1},\ldots,w_{a_n}] &= \log \prod_{d\in\mathcal{D}_n} |\Psi_d(\alpha_1,\beta_1)| + O\left(\log \prod_{k=1}^n \delta_{a_k}\right) \\ &= \log|\alpha_1| \sum_{d\in\mathcal{D}_n} \phi(d) + O\left(E_1(n)\right) \\ &+ O\left(\sum_{d\in\mathcal{D}_n} \tau(d)\log(d+1)\right) \\ &= \log|\alpha_1| A_2(n) + O(E_2(n)), \end{aligned} \tag{15}$$

where we write

$$A_2(n) = \sum_{d\in\mathcal{D}_n} \phi(d) \quad \text{and} \quad E_2(n) = \sum_{k=1}^n \tau(a_k)^2 \log(a_k+1). \tag{16}$$

The last error term in (15) comes from the fact that every a_k for $k = 1, \ldots, n$ contributes at most $\tau(a_k)$ members $d \in \mathcal{D}_n$ and for each one of them we have

$$\tau(d) \log(d+1) \le \tau(a_k) \log(a_k + 1).$$

All this has been obtained without any arithmetic condition on the sequence $(a_n)_{n\ge 1}$. Let us see some examples.

3 Examples

3.1 The case of the sequences $a_n = \phi(n)$ and $a_n = \sigma(n)$

Both sequences have almost linear growth, that is the inequality $a_n \le n^{1+o(1)}$ holds for both sequences as $n \to \infty$, therefore both inequalities

$$E_1(n) \le n^{1+o(1)} \quad \text{and} \quad E_2(n) \le n^{1+o(1)}$$

hold as n tends to infinity. Further,

$$A_1(n) = c_{\mathbf{a}} n^2 + O(n \log n),$$

with $c_{\mathbf{a}} = 3/\pi^2$ or $\pi^2/12$ according to whether $a_n = \phi(n)$ or $a_n = \sigma(n)$, respectively. As for $\mathcal{D}_n$, we cut it into two parts:

$$\mathcal{D}_{1,n} = \{d \in \mathcal{D}_n \mid 1 \le d \le n/(\log n)^{1/4}\}.$$

Here we use the trivial estimate

$$\sum_{d \in \mathcal{D}_{1,n}} \phi(d) \le \sum_{d \le n/(\log n)^{1/4}} d = O\left(\frac{n^2}{(\log n)^{1/2}}\right).$$

Put $\mathcal{D}_{2,n} = \mathcal{D}_n \backslash \mathcal{D}_{1,n}$. If $d \in \mathcal{D}_{1,n}$, we then have that $d = \phi(u)/v$, where $u \le n$ and $v \le (\log n)^{1/4}$ in case when $a_k = \phi(k)$. When $a_k = \sigma(k)$, we have $d = \sigma(u)/v$ for some $u \le n$, where $v \le c_1(\log n)^{1/4} \log\log n$ for some constant c_1. Here, we use the fact that $\sigma(u) \le c_1 u \log\log u$ holds for all $u \ge 3$ with some constant c_1. Each one of the sets $\{\phi(u) \le n\}$ and $\{\sigma(u) \le c_1 n \log\log n\}$ has $O(n/(\log n)^{1-\varepsilon})$ elements, (see [5] or Theorems 1 and 14 in [7]), where $\varepsilon > 0$ can be taken to be as small as we wish and will be fixed later. Thus,

$$\#\mathcal{D}_{2,n} = O\left(\frac{n \log\log n}{(\log n)^{3/4-\varepsilon}}\right) = O\left(\frac{n}{(\log n)^{1/2}}\right)$$

provided that we choose $\varepsilon = 1/10$. Hence,

$$\sum_{d \in \mathcal{D}_{2,n}} \phi(d) \le n \# \mathcal{D}_{2,n} = O\left(\frac{n^2}{(\log n)^{1/2}}\right),$$

and we get the estimate

$$\frac{\log |u_{a_1} u_{a_2} \cdots u_{a_n}|}{\log \operatorname{lcm}[u_{a_1}, u_{a_2}, \ldots, u_{a_n}]} \gg \sqrt{\log n}.$$

In particular,

$$\log \operatorname{lcm}[u_{a_1}, u_{a_2}, \ldots, u_{a_n}] = o\left(\log |u_{a_1} u_{a_2} \cdots u_{a_n}|\right) \quad \text{as} \quad n \to \infty,$$

a phenomenon that does not happen with the sequences dealt with in [2].

We record this as the following result.

Theorem 3. *If $a_n = \phi(n)$ for all $n \ge 1$, then*

$$\log \operatorname{lcm}[u_{a_1}, u_{a_2}, \ldots, u_{a_n}] = o\left(\log |u_{a_1} u_{a_2} \cdots u_{a_n}|\right) \quad \text{as} \quad n \to \infty.$$

The same conclusion holds when $a_n = \sigma(n)$ for all $n \ge 1$.

3.2 The case of the sequences $a_n = |b_n|$ with $(b_n)_{n\ge1}$ binary recurrent

Since we are working very generally, we shall assume that

$$b_{n+2} = C b_{n+1} + D b_n,$$

where C and D are nonzero integers such that the equation $\lambda^2 - C\lambda - D = 0$ has two distinct roots γ, δ with γ/δ not a root of 1. Then

$$b_n = \eta \gamma^n + \zeta \delta^n,$$

with some nonzero algebraic numbers η, ζ in $\mathbb{K} = \mathbb{Q}(\gamma)$. We assume that $|\gamma| \ge |\delta|$. Thus,

$$A_1(n) = \sum_{k=1}^{n} |b_n|.$$

We also assume that we work only with the numbers $k = 1, \ldots, n$, such that $b_k \ne 0$. It is easy to see that if such k with $b_k = 0$ exists, then it is unique. Indeed, for if not, then say $b_{k_1} = b_{k_2} = 0$ for integers $k_1 < k_2$.

Regarding these two equations as a degenerate homogeneous linear system in the unknowns $\eta,\ \zeta$ whose coefficient matrix is

$$\begin{pmatrix} \gamma^{k_1} & \delta^{k_1} \\ \gamma^{k_2} & \delta^{k_2} \end{pmatrix},$$

we get that $(\gamma/\delta)^{k_2-k_1}=1$, which is not allowed because γ/δ is not a root of unity. By Baker's bound,

$$A_1(n) \ge |b_n| = \exp(n\log|\gamma| + O(\log n)). \tag{17}$$

This gives us the main term for $\log|u_{a_1}u_{a_2}\cdots a_{a_n}|$. It remains to study $\log \mathrm{lcm}[u_{a_1},\ldots,u_{a_n}]$. Clearly,

$$E_1(n) = \exp(o(n)) \quad \text{and} \quad E_2(n) = \exp(o(n)) \quad \text{as} \quad n\to\infty.$$

To get $A_2(n)$, we put $T_1=\gcd(C^2,D)$, $\gamma_1=\gamma^2/T_1,\ \delta_1=\delta^2/T_1$ and

$$b_n = T_1^{\lfloor n/2\rfloor} z_n,$$

where

$$z_n = \eta_1\gamma_1^{\lfloor n/2\rfloor} + \zeta_1\delta_1^{\lfloor n/2\rfloor} \quad \text{with} \quad (\eta_1,\zeta_1) = \begin{cases} (\eta,\zeta) & \text{if} \quad n\equiv 0 \pmod 2, \\ (\eta\gamma,\zeta\delta) & \text{if} \quad n\equiv 1 \pmod 2. \end{cases}$$

Let $\mathcal{T}$ be the finite set of primes sitting above some prime ideal π from $\mathcal{O}_{\mathbb{K}}$ which appears with nonzero exponent in the factorization of one of the principal fractional ideals generated by $\gamma,\ \delta,\ \eta,\ \zeta,\ \gamma-\delta$ in $\mathbb{K}$. We split $\mathcal{D}_n$ into three subsets as follows. We take

$$\mathcal{D}_{1,n} = \{d\in\mathcal{D}_n \mid d \le |\gamma|^{n/2}\}.$$

Since $d\mid a_k$ for some $k=1,\ldots,n$ and since each a_k has $a_k^{o(1)}=\exp(o(n))$ divisors as $n\to\infty$, we get

$$\sum_{d\in\mathcal{D}_{1,n}} \phi(d) = O\left(n|\gamma|^{n/2}\exp(o(n))\right) \le |\gamma|^{(1/2+o(1))n} \quad \text{as} \quad n\to\infty. \tag{18}$$

Next we take

$$\mathcal{D}_{2,n} = \{d\in\mathcal{D}_n\backslash\mathcal{D}_{1,n} : d\mid a_i \text{ and } d\mid a_j \text{ for some } i<j\in\{1,\ldots,n\}\}.$$

Since $d>|\gamma|^{n/2}$ and $a_k=O(|\gamma|^k)$ holds for both $k=i$ and j, it follows that $i\ge n/2+O(1)$, therefore

$$j-i \le n/2 + O(1).$$

Now write $d = d_1 d_2$, where d_1 is the contribution to d from primes coming from $\mathcal{T}$ and d_2 is the contribution to d of the remaining primes. Since γ_1 and δ_1 are coprime, it follows, again by the theory of linear forms in p-adic logarithms, that $\mu_p(c_m) < c(p)\log(m+1)$ holds for all primes p with some constant c_p depending on p. This shows that

$$\log d_1 = \left(\frac{\log T_1}{2}\right) n + O(\log(n+1)).$$

As for d_2, we have that $d_2 \mid z_i$ and $d_2 \mid z_j$. Since η and δ are invertible modulo d_2, we get that

$$\left(\frac{\gamma}{\delta}\right)^i \equiv -\frac{\zeta}{\eta} \pmod{z_2} \qquad \text{and} \qquad \left(\frac{\gamma}{\delta}\right)^j \equiv -\frac{\zeta}{\eta} \pmod{z_2},$$

from where we deduce that

$$\left(\frac{\gamma}{\zeta}\right)^{j-i} \equiv 1 \pmod{z_2}.$$

Thus, z_2 divides the sth term of the Lucas sequence $(\gamma^s - \delta^s)/(\gamma - \delta)$ with $s = j - i \le n/2 + O(1)$. Each of such terms has $\exp(o(n))$ divisors as $n \to \infty$, and there are only $O(n)$ possibilities for s. Hence,

$$\sum_{d \in \mathcal{D}_{2,n}} \phi(d) \le n|\gamma|^{n/2} \exp(o(n)) = |\gamma|^{(1/2+o(1))n} \quad \text{as} \quad n \to \infty. \tag{19}$$

Finally, look at numbers $d \in \mathcal{D}_{3,n} = \mathcal{D}_n \backslash (\mathcal{D}_{1,n} \cup \mathcal{D}_{2,n})$. Each one of these numbers divides a unique $a_k = k_d$ and they are all $> |\gamma|^{n/2}$. Further, each number $d > |\gamma|^{n/2}$ which divides a_k for some k is either in $\mathcal{D}_{3,n}$ or in $\mathcal{D}_{2,n}$. Using the formula

$$m = \sum_{d \mid m} \phi(d)$$

and adding into our sums also all the divisors $d \le |\gamma|^{n/2}$ of all the numbers a_k for $k \in \{1, \ldots, n\}$ (at most n values for k, at most $\exp(o(n))$ as $n \to \infty$ values for d for each k, and none exceeding $|\gamma|^{n/2}$), we get easily that

$$\sum_{d \in \mathcal{D}_{3,n}} \phi(d) = \sum_{k=1}^{n} a_k + O\left(n|\gamma|^{n/2+o(n)} \exp(o(n))\right) = A_1(n) + O\left(|\gamma|^{n/2+o(n)}\right). \tag{20}$$

Putting everything together from (18), (19), (20) and using also (17), we get that

$$A_2(n) = \sum_{k=1}^{3} \sum_{d \in \mathcal{D}_{k,n}} \phi(d) = A_1(n) + O\left(|\gamma|^{n/2+o(n)}\right) = (1+o(1))A_1(n),$$

which leads to the conclusion that in this case quite the opposite of what had happened in the previous case holds, namely

$$\log \operatorname{lcm}[u_{a_1}, u_{a_2}, \ldots, u_{a_n}] = (1+o(1)) \log |u_{a_1} u_{a_2} \cdots u_{a_n}| \quad \text{as} \quad n \to \infty.$$

Further, note that the expression for $A_1(n)$ can be simplified when $|\gamma| > |\delta|$ (that is, when both γ and δ are real), since then

$$|a_n| = |\eta||\gamma|^n + O(|\delta|^n) \quad \text{holds for all} \quad n \geq 1,$$

therefore

$$A_1(n) = \left(\frac{|\eta\gamma|}{|\gamma|-1}\right)|\gamma|^n + O(|\gamma|^{c_2 n}),$$

where c_2 is any constant satisfying $\log|\delta|/\log|\gamma| < c_2 < 1$.

We record the following result.

Theorem 4. *If $a_n = |b_n|$, where $(b_n)_{n\geq 1}$ is a non-degenerate binary recurrence, then*

$$\log \operatorname{lcm}[u_{a_1}, u_{a_2}, \ldots, u_{a_n}] = (1+o(1)) \log |u_{a_1} u_{a_2} \cdots u_{a_n}| \quad \textit{as} \quad n \to \infty.$$

3.3 The case of the Lucas sequence of the second kind

Jones and Kiss [12], studied the least common multiple of the sequence u_{mn}/u_n for $m > 0$. For completeness, we study the case for $m = 2$ directly by our method which will give us a good comparison. Thus $(u_n)_{n\geq 1}$ is replaced by $(L_n)_{n\geq 1}$ given by $L_0 = 2,\ L_1 = A$. In this case, the analog of formula (1) is

$$L_n = \alpha^n + \beta^n.$$

By Baker's method, we have again

$$|L_m| = \exp(m \log|\alpha| + O(\log(m+1)),$$

so formula (3) holds for this case also:

$$\log|L_{a_1} L_{a_2} \cdots L_{a_n}| = \log|\alpha| A_1(n) + O\left(E_1(n)\right). \tag{21}$$

It remains to estimate the least common multiple. The analogue of formula (6) is

$$L_n = \begin{cases} T^{(n-1)/2} A w_{2n}/w_n & \text{if} \quad n \equiv 1 \pmod 2, \\ A u_1 T^{n/2} w_{2n}/w_n & \text{if} \quad n \equiv 0 \pmod 2. \end{cases} \tag{22}$$

We now get that the analogues of formulas (7) and (8) are

$$\text{lcm}[L_{a_1}, L_{a_2}, \ldots, L_{a_n}] =: M_1 M_2, \tag{23}$$

where again M_1 is the contribution to the above least common multiple of the primes from $\mathcal{S}$ and M_2 is the contribution of the remaining primes, then we have

$$\begin{aligned} \log M_1 &= \left(\frac{\log T}{2}\right) \max\{a_k\}_{1 \le k \le n} + O\left(E_1(n)\right), \\ \log M_2 &= \log \text{lcm}[w_{2a_1}/w_{a_1}, \ldots, w_{2a_n}/w_{a_n}] + O\left(E_1(n)\right). \end{aligned} \tag{24}$$

Now observe that by cyclotomicity, we have that

$$\frac{w_{2m}}{w_m} = \delta_{2m} \delta_m^{-1} \prod_{\substack{d \mid 2m \\ d \nmid m}} \Psi_d(\alpha_1, \beta_1),$$

and now the previous argument shows that if we put

$$\mathcal{D}'_n = \{d : d \mid 2a_k \text{ but } d \nmid a_k \text{ for some } k \in \{1, \ldots, n\}\},$$

then in fact

$$\log \text{lcm}[w_{2a_1}/w_{a_1}, \ldots, w_{2a_n}/w_{a_n}] = \log |\alpha_1| A_3(n) + O(E_2(n)),$$

where

$$A_3(n) = \sum_{d \in \mathcal{D}'_n} \phi(d).$$

As a concluding example, take $a_k = k$. Then

$$A_1(n) = \sum_{k \le n} k = \frac{n^2}{2} + O(n).$$

Clearly,

$$E_1(n) \le \sum_{k \le n} \log(k+1) = O(n \log n).$$

Next

$$\log M_1 = \left(\frac{T}{2}\right) n + O(E_1(n)) = O(n \log n),$$

and

$$\log M_2 = \log |\alpha_1| A_3(n) + O(E_2(n)),$$

where

$$A_3(n) = \sum_{d \in \mathcal{D}'_n} \phi(d),$$

and

$$\mathcal{D}'_n = \{2, 4, \ldots, 2n\}.$$

Observe that $\mathcal{D}'_n$ is the set of even numbers less than or equal to $2n$. So,

$$A_3(n) = \sum_{\substack{d \equiv 0 \pmod 2 \\ d \leq 2n}} \phi(d) = \sum_{d \leq 2n} \phi(d) - \sum_{1 \leq k \leq n} \phi(2k-1) := S_1 + S_2.$$

Clearly,

$$S_1 = \frac{(2n)^2}{2\zeta(2)} + O(n \log n) = \frac{2n^2}{\zeta(2)} + O(n \log n).$$

It is well-known that if $f(x) \in \mathbb{Z}[x]$ is a polynomial with integer coefficients of degree h with leading coefficient a_h, then

$$\sum_{k \leq n} \phi(f(k)) = c_f a_h (h+1)^{-1} n^{h+1} + O(n^h \log n),$$

with

$$c_f = \sum_{k=1}^{\infty} \frac{\mu(k) \rho_f(k)}{k^2},$$

where $\rho_f(n)$ is the number of $x \pmod k$ of the congruence $f(x) \equiv 0 \pmod k$ (see [18]). For the particular case of the polynomial $f(x) = 2x - 1$, we have $\rho_f(k) = 1$ if k is odd and $\rho_f(k) = 0$ if k is even, so

$$c_f = \sum_{k \equiv 1 \pmod 2} \frac{\mu(k)}{k^2} = \prod_{p \geq 3} \left(1 - \frac{1}{p^2}\right) = \frac{4}{3\zeta(2)},$$

so since $h = 1,\ a_h = 2$, we have

$$S_2 = \frac{4n^2}{3\zeta(2)} + O(n \log n),$$

leading to

$$A_3(n) = \left(2 - \frac{4}{3}\right) \frac{n^2}{\zeta(2)} + O(n \log n) = \frac{2n^2}{3\zeta(2)} + O(n \log n).$$

Unfortunately, given that our method is so general, the error terms are not very good, and are worse than the ones obtained in [1] and [2], for example. That is, for our particular case, we have

$$E_2(n) \le \sum_{d \le 2n} \tau(d)^2 \log(d+1) = O(n(\log n)^5),$$

so that

$$\log \operatorname{lcm}[L_1, L_2, \cdots, L_n] = \log M_1 + \log M_2 = \left(\frac{2 \log |\alpha_1|}{3\zeta(2)}\right) n^2 + O(n(\log n)^5).$$

We get that the analogue of the result from (2) for the Lucas sequence of the second kind is

$$\begin{aligned} \frac{\log |L_1 L_2 \cdots L_n|}{\log \operatorname{lcm}[L_1, L_2, \ldots, L_n]} &= \frac{(\log |\alpha|)/2}{(2|\log |\alpha_1|/(3\zeta(2))} + O\left(\frac{(\log n)^5}{n}\right) \\ &= \frac{3\zeta(2)}{4(1-\kappa)} + O\left(\frac{(\log n)^5}{n}\right). \end{aligned}$$

We record this as follows.

Theorem 5. *We have*

$$\frac{\log |L_1 L_2 \cdots L_n|}{\log \operatorname{lcm}[L_1, L_2, \ldots, L_n]} = \frac{3\zeta(2)}{4(1-\kappa)} + O\left(\frac{(\log n)^5}{n}\right).$$

Here, the error term is slightly worse than in [12] because of our general approach.

3.4 The case when $a_k = f(k)$ with a polynomial $f(X) \in \mathbb{Z}[X]$

In this section, we treat the case when $a_k = |f(k)|$, with $f(X) \in \mathbb{Z}[X]$, a polynomial with integer coefficients. Say

$$f(X) = C_0 X^m + C_1 X^{m-1} + \cdots + C_m \in \mathbb{Z}[X]$$

has degree $m \geq 1$. We assume that $C_0 > 0$. As in previous cases, we only work with numbers k such that $f(k) \neq 0$. Clearly, the equation $f(k) = 0$ has at most m solutions k. We have

$$\begin{aligned} A_1(n) &= \sum_{1 \leq k \leq n} |f(k)| = \frac{C_0}{m+1} n^{m+1} + O(n^m) \\ E_1(n) &= \sum_{1 \leq k \leq n} \log(|f(k)| + 1) = O(n \log n), \end{aligned}$$

so, by (3), we have

$$\log \left| \prod_{\substack{1 \leq k \leq n \\ a_k \neq 0}} u_{a_k} \right| = \left(\frac{C_0 \log |\alpha|}{(m+1)} \right) n^{m+1} + O(n^m \log n). \qquad (25)$$

To get $A_2(n)$, first we put $C = \gcd(C_0, \ldots, C_m)$ and write $f(X) = Cg(X)$. Further, putting $\alpha_0 = \alpha^C$, $\beta_0 = \beta^C$ and

$$v_k = \frac{\alpha_0^k - \beta_0^k}{\alpha_0 - \beta_0} \quad \text{for} \quad k \geq 0,$$

we have

$$u_{a_k} = \frac{\alpha^{f(k)} - \beta^{f(k)}}{\alpha - \beta} = \frac{\alpha_0^{g(k)} - \beta_0^{g(k)}}{\alpha_0 - \beta_0} u_C = v_{g(k)} u_C.$$

Thus, instead of working with the sequences $\{u_n\}_{n \geq 1}$ and $a_k = |f(k)|$ for $1 \leq k \leq n$, we can work with $\{u_C v_n\}_{n \geq 1}$ and $b_k = |g(k)|$ for $1 \leq k \leq n$. The characteristic equation for the sequence $\{u_C v_n\}_{n \geq 1}$ is

$$X^2 - A_0 X - B_0 = 0,$$

where $A_0 = \alpha^C + \beta^C = u_{2C}/u_C$ and $B_0 = -(\alpha\beta)^C = (-1)^{C-1} B^C$. The Lehmer sequence $\{w_n\}_{n \geq 0}$ associated to $\{v_n\}_{n \geq 0}$ is given by formula (5) with the roots $\alpha_1 = \alpha_0/\sqrt{T_0}$, $\beta_1 = \beta_0/\sqrt{T_0}$, where $T_0 = \gcd(A_0^2, B_0)$. The arguments from the beginning of Section 2 show that

$$\operatorname{lcm}[u_{a_1}, \ldots, u_{a_n}] = M_1 M_2,$$

where

$$\begin{aligned} M_1 &= \left(\frac{\log T_0}{2} \right) \max\{|g(k)|\}_{1 \leq k \leq n} + O(E_1(n)) \\ M_2 &= \log \operatorname{lcm}[w_{b_1}, \ldots, w_{b_k}] + O(E_1(n)). \end{aligned}$$

Clearly,

$$M_1 = O(n^m \log n).$$

By formula (15), we have

$$M_2 = \log|\alpha_1| A_2(n) + O(E_2(n)),$$

where

$$A_2(n) = \sum_{d\in\mathcal{D}_n} \phi(d) \quad \text{and} \quad E_2(n) = \sum_{k\le n} \tau(b_k)^2 \log(b_k+1),$$

and

$$\mathcal{D}_n = \{d \mid g(k) \text{ for some } k \in [1,n] \text{ with } g(k) \neq 0\}.$$

By a result of van der Corput (see [20]), we have

$$\sum_{\substack{1\le k\le n\\ g(k)\neq 0}} \tau(|g(k)|)^i = O(n(\log n)^{c(i)}) \tag{26}$$

for all positive integers i, where $c(i)$ is some constant depending on i and g. We put $c_1 = \max\{c(1), m\}$ and $c_2 = c(2)$. In particular, from the above estimate (26) with $i = 2$ we get

$$E_2(n) = O\left(\log n \sum_{\substack{1\le k\le n\\ g(k)\neq 0}} \tau(|g(k)|)^2\right) = O(n(\log n)^{c_2+1}).$$

It remains to understand $A_2(n)$. For this, we split the set $\mathcal{D}_n$ into three subsets according to whether d is small, or k is small, or both are large.

We put

$$\mathcal{D}_{1,n} = \{d \in \mathcal{D}_n : d \le n^m/(\log n)^{c_1+1}\}.$$

Then

$$\sum_{d\in\mathcal{D}_{1,n}} \phi(d) \le \frac{n^m \#\mathcal{D}_n}{(\log n)^{c_1+1}} \le \frac{n^m}{(\log n)^{c_1+1}} \sum_{\substack{1\le k\le n\\ g(k)\neq 0}} \tau(|g(k)|) = O\left(\frac{n^{m+1}}{\log n}\right). \tag{27}$$

Next, let

$$D_{2,n} = \{d \mid g(k) \text{ for some } k \le n/(\log n)^{c_1+1} \text{ with } g(k) \neq 0\}.$$

Then

$$\sum_{d\in\mathcal{D}_{2,n}} \phi(d) \le \max\{|g(k)|\}_{k\le n/(\log n)^{c_1+1}} \#\mathcal{D}_n = O\left(\frac{n^{m+1}}{\log n}\right). \tag{28}$$

We now look at the numbers $d \in \mathcal{D}_n\backslash(\mathcal{D}_{1,n} \cup \mathcal{D}_{2,n})$. Since $|g(k)| \le c_3 k^m$ holds for all $k \ge 1$ with some constant c_3, we conclude that we may write $d = |g(k)|/e$, where $n/(\log n)^{c_1+1} \le k \le n$ and $1 \le e \le c_3(\log n)^{c_1+1}$. Furthermore, since $C_0 > 0$ and $k > n/(\log n)^{c_1+1}$, it follows that for large enough n, the number $g(k)$ is positive. So, from now on we shall simply write $g(k)$ for such k instead of $|g(k)|$. Put $\mathcal{K}_n = [n/(\log n)^{c_1+1}, n]$ and $\mathcal{E}_n = [1, c_3(\log n)^{c_1+1}]$.

It turns out that from here on the argument (and indeed, the answer), splits into two cases according to whether $g(X)$ (or $f(X)$) has at least two distinct roots, or not.

3.4.1 Proof of Theorem 1

We start with a preliminary result about polynomials satisfying a certain functional equation.

Lemma 1. *Let $f(X) \in \mathbb{C}[X]$ of degree m and $r \neq 0$, s, η be complex numbers with r not a root of unity such that*

$$f(rX + s) = \eta f(X). \tag{29}$$

Then $f(X) = (aX + b)^m$ for some complex numbers a and b such that $as = b(r - 1)$.

Proof. Identifying the leading coefficient in equation (29), we get $\eta = r^m$. We prove the lemma by induction on m. For $m = 1$, $f(X) = aX + b$, so the relation $f(rX + s) = f(X)$ gives $a(rX + s) + b = r(aX + b)$, so $as = b(r - 1)$, as we requested. Assume now that $m \ge 2$ and that the claim is true for polynomials of degree smaller than m and let $f(X)$ be a polynomial of degree m such that $f(rX + s) = r^m f(X)$. Taking derivates, we get $f'(rX + s) = r^{m-1} f'(X)$, so, by the induction hypothesis, we have $f'(X) = (aX + b)^{m-1}$ where $as = b(r - 1)$. Thus, $f(X) = \frac{1}{m}(aX + b)^m + d$ for some number d. But then the relation (29) becomes

$$\frac{1}{m}(a(rX + s) + b)^m + d = \frac{r^m}{m}(aX + b)^m + r^m d.$$

Since $a(rX+s)+b = arX+as+b = r(aX+b)$, it follows that we must have $d = r^m d$, so $d(r^m - 1) = 0$, so $d = 0$, because r is not a root of unity. We thus get that $f(X) = (a_1X + b_1)^m$, where $a_1 = a/m^{1/m}$, $b_1 = b/m^{1/m}$. $\square$

We next have the following lemma.

Lemma 2. *There exists a constant c_4 such that for $n > n_0$ the number of solutions $(k_1, k_2, e_1, e_2) \in \mathcal{K}_n^2 \times \mathcal{E}_n^2$ with $k_1 \neq k_2$ of the equation*

$$\frac{g(k_1)}{e_1} = \frac{g(k_2)}{e_2} \tag{30}$$

is at most $(\log n)^{c_4}$.

Proof. Observe first that if $e_1 = e_2$, then $g(k_1) = g(k_2)$. However, for large n, $g'(k)$ if positive for all $k > n/(\log n)^{c_1+1}$, and in particular $g(k)$ is increasing for $k \in \mathcal{K}_n$, so the above equation implies $k_1 = k_2$, which is not allowed. Thus, for large n, any solution (k_1, k_2, e_1, e_2) will have $e_1 \neq e_2$. Write

$$g(X) = C_0' X^m + C_1' X^{m-1} + \cdots + C_m', \quad \text{where} \quad C_i' = C_i/C \quad (i = 0, \ldots, m).$$

Observe that

$$C_0'^{m-1} m^m g(X) = (C_0' m X + C_1')^m + h(X),$$

where $h(X) \in \mathbb{Z}[X]$ is of degree at most $m - 2$. Thus, from equation (30) we get

$$\begin{aligned} C_0'^{m-1} m^m (e_2 g(k_1) - e_1 g(k_2)) &= e_2 (C_0' m k_1 + C_1')^m - e_1 (C_0' m k_2 + C_1')^m \\ &+ e_2 h(k_1) - e_1 h(k_2) = 0, \end{aligned}$$

therefore if we put $\ell(X) = C_0' m X + C_1'$ and $\ell_i = \ell(k_i)$ for $i = 1, 2$, then

$$|e_2 \ell_1^m - e_1 \ell_2^m| = O(e_1 k_2^{m-2} + e_2 k_1^{m-2}) = O(n^{m-2} (\log n)^{c_1+1}). \tag{31}$$

The left–hand side above equals

$$\prod_{\zeta^m = 1} |e_1^{1/m} \ell_1 - \zeta e_2^{1/m} \ell_2|, \tag{32}$$

where $e_1^{1/m}$ and $e_2^{1/m}$ stand for the real positive roots of order m of e_1 and e_2 respectively. If ζ is complex nonreal root of unity of order m, then

$$|e_1^{1/m} \ell_1 - \zeta e_2^{1/m} \ell_2| \geq |\mathrm{Im}(\zeta)| e_2^{1/m} \ell_2 \gg \frac{n}{(\log n)^{c_1+1}}, \tag{33}$$

and a similar inequality holds when $\zeta = -1$ and m is even. Thus, using inequality (33) to bound from below all factors from the product (32) except for the one corresponding to $\zeta = 1$, and comparing the inequality obtained in this way with (31), we get

$$|e_1^{1/m}\ell_1 - e_2^{1/m}\ell_2| \ll \frac{(\log n)^{c_5}}{n},$$

where $c_5 = mc_1 + m$. In particular,

$$\left|\alpha(e_1, e_2) - \frac{\ell_2}{\ell_1}\right| \ll \frac{(\log n)^{c_5}}{\ell_1^2},$$

where $\alpha(e_1, e_2) = (e_1/e_2)^{1/m}$. Write $\delta = \gcd(\ell_1, \ell_2)$, $\ell_1 = \delta m_1$, $\ell_2 = \delta m_2$. We then get that

$$\left|\alpha(e_1, e_2) - \frac{m_2}{m_1}\right| < \frac{c_6(\log n)^{c_5}}{\delta^2 m_1^2}, \tag{34}$$

where c_6 is some positive constant. Suppose first that $\delta^2 < 2c_6(\log n)^{c_5}$. Then δ can take only $O((\log n)^{c_5/2})$ positive integer values. By a result of Worley [21], inequality (34) implies that

$$\frac{m_1}{m_2} = \frac{ap_k + bp_{k-1}}{aq_k + bq_{k-1}}, \quad \text{or} \quad \frac{ap_{k+1} + bp_{k-1}}{aq_{k+1} + bq_{k-1}}$$

for some integers $k \geq 1$, $a \geq 1$ and b with $a|b| < 2c_6(\log n)^{c_5}$, where $\{p_k/q_k\}_{k\geq 0}$ is the kth convergent to $\alpha(e_1, e_2)$. Since $\max\{m_1, m_2\} \leq n$, we have $k = O(\log n)$ uniformly in e_1 and e_2. Since there are $O((\log n)^{2c_1+2})$ choices for the pair (e_1, e_2); hence, for the number $\alpha(e_1, e_2)$, $O((\log n)^{c_5/2})$ choices for δ, and then $O((\log n)^{2c_5+1})$ choices for the triple (a, b, k), we get a totality of $O((\log n)^{2c_1+2.5c_5+3})$ choices for (ℓ_1, ℓ_2); hence, for (k_1, k_2), in this instance. Assume next that $\delta > 2c_6(\log n)^{c_5}$. We then have

$$\left|\alpha(e_1, e_2) - \frac{m_2}{m_1}\right| < \frac{1}{2m_1^2}.$$

Either $\alpha(e_1, e_2) = m_2/m_1$ is rational, so the expression on the left above is 0, or $\alpha(e_1, e_2)$ is irrational and $m_2/m_1 = p_k/q_k$ is a convergent to $\alpha(e_1, e_2)$ by a criterion of Legendre. Here, as before, $k = O(\log n)$. Fix e_1, e_2, m_1, m_2. Then

$$\frac{m_1}{m_2} = \frac{\ell_1}{\ell_2} = \frac{C_0' m k_1 + C_1'}{C_0' m k_2 + C_1'},$$

so

$$k_2 = rk_1 + s, \quad \text{where} \quad r = \frac{m_2}{m_1} \quad \text{and} \quad s = \frac{C_1'(m_2 - m_1)}{C_0' m m_1}.$$

Note that $r \neq 1$, because if not, then $m_1 = m_2 = 1$, so $k_2 = k_1$, which is not allowed. Since r is also positive, it follows that r is not a root of unity. Going back to relation (30), we get

$$\frac{g(rk_1+s)}{g(k_1)} = \eta \qquad \text{with} \qquad \eta = \frac{e_2}{e_1}.$$

Since r, s, η are fixed, the above relation is a polynomial relation in k_1, so it has at most m roots, unless the rational function $g(rX+s)/g(X)$ is constant η, which is not the case by Lemma 1 and the fact that $g(X)$ has at least two distinct zeros. Thus, when e_1, e_2, m_1, m_2 are fixed, there are at most m possibilities for k_1, and then k_2 is uniquely determined. This shows that the number of solutions of equation (30) in this case is $O((\log n)^{2c_1+3})$. The lemma now follows with $c_4 = 2c_1 + 2.5c_5 + 4 = (2.5m+2)c_1 + 2.5m + 4$. $\square$

For each $d \in \mathcal{D}_n \backslash (\mathcal{D}_{1,n} \cup \mathcal{D}_{2,n})$ let $r(d)$ be the number of representations of d under the form $d = g(k)/e$ for some $k \in \mathcal{K}_n$ and $e \in \mathcal{E}_n$. Lemma 2 shows that if we put

$$\mathcal{D}_{3,n} = \{d \in \mathcal{D}_n \backslash (\mathcal{D}_{1,n} \cup \mathcal{D}_{2,n}) : r(d) > 1\},$$

then

$$\#\mathcal{D}_{3,n} = O((\log n)^{c_4}). \tag{35}$$

We now use the relation

$$m = \sum_{d|m} \phi(d)$$

with $m = g(k)$ in the following way:

$$g(k) = \sum_{\substack{e|g(k)\\ e\in\mathcal{E}_n}} \phi(g(k)/e) + O\left(g(k) \sum_{\substack{e|g(k)\\ e>c_3(\log n)^{c_1+1}}} \frac{1}{e} \right), \tag{36}$$

which we rewrite as

$$g(k) = \sum_{\substack{e|g(k)\\ e\in\mathcal{E}_n}} \phi(g(k)/e) + O\left(n^m \sum_{\substack{e|g(k)\\ e>c_3(\log n)^{c_1+1}}} \frac{1}{e} \right). \tag{37}$$

We sum up the above relation for all $k \in \mathcal{K}_n$ getting

$$\begin{aligned}\sum_{k\in\mathcal{K}_n} g(k) &= \sum_{d\in\mathcal{D}_n\setminus(\mathcal{D}_{1,n}\cup\mathcal{D}_{2,n})} \phi(d) + O(n^m(\#\mathcal{D}_{3,n})^2)\\ &+ O\left(n^m \sum_{e>c_3(\log n)^{c_1+1}} \frac{1}{e} \sum_{\substack{k\in\mathcal{K}_n\\ g(k)\equiv 0 \pmod e}} 1\right). \end{aligned} \tag{38}$$

The term on the left in (38) is obviously

$$\sum_{k\in\mathcal{K}_n} (C_0' k^m + O(k^{m-1})) = \frac{C_0' n^{m+1}}{m+1} + O\left(\frac{n^{m+1}}{\log n}\right).$$

The first term on the right in (38) is

$$A_2(n) - \sum_{d\in\mathcal{D}_{1,n}\cup\mathcal{D}_{2,n}} \phi(d) = A_2(n) + O\left(\frac{n^{m+1}}{\log n}\right),$$

by estimates (27) and (28). The second term on the right in (38) is of order $O(n^m(\log n)^{2c_4})$ by (35). For the last term on the right in (38), we use the fact that

$$\sum_{\substack{k\in\mathcal{K}_n\\ g(k)\equiv 0 \pmod e}} 1 = \rho_g(e)\left\lfloor \frac{\#\mathcal{K}_n}{e}\right\rfloor + O(\rho_g(e)) \ll \begin{cases} \frac{n\rho_g(e)}{e} & \text{if} \quad e\le n,\\ \rho_g(e) & \text{if} \quad e>n,\end{cases}$$

where ρ_g has the same meaning as in Section 3.3. We thus get that the last term on the right in (38) is of order

$$n^{m+1} \sum_{c_3(\log n)^{c_1+1}<e\le n} \frac{\rho_g(e)}{e^2} + n^m \sum_{\substack{n<e\\ e|g(k) \text{ for some } k\in\mathcal{K}_n}} \frac{\rho_g(e)}{e} := S_1 + S_2.$$

From the Ore–Nagell theorem (see [16]), we have $\rho_g(e) \ll m^{\omega(e)}$. Thus,

$$\begin{aligned}
S_1 &= \frac{n^{m+1}}{(\log n)^{c_1+1}} \sum_{e\le n} \frac{\rho_g(e)}{e} \ll \frac{n^{m+1}}{(\log n)^{c_1+1}} \sum_{e\le n} \frac{m^{\omega(e)}}{e} \\
&= \frac{n^{m+1}}{(\log n)^{c_1+1}} \prod_{p\le n} \left(1+\frac{m}{p}+\frac{m}{p^2}+\cdots\right) \\
&\ll \frac{n^{m+1}}{(\log n)^{m+1}} \exp\left(\sum_{p\le n} \frac{m}{p} + O(1)\right) \\
&\ll \frac{n^{m+1}}{(\log n)^{c_1+1}} \exp(m\log\log n + O(1)) \\
&\ll \frac{n^{m+1}}{(\log n)^{c_1+1-m}} = O\left(\frac{n^{m+1}}{\log n}\right).
\end{aligned}$$

Here, we used the fact that $c_1 \ge m$.

For S_2, we use the estimate $\omega(e) = o(\log e)$ as $e \to \infty$, to conclude that $\rho_g(e) \le m^{o(\log e)} = e^{o(1)}$ as $e \to \infty$. In particular, $\rho(e) < e^{1/2}$ for all $e > n$ and n sufficiently large. Thus,

$$\begin{aligned}
S_2 &\ll n^m \sum_{\substack{n<e \\ e\mid g(k) \text{ for some } k\in\mathcal{K}_n}} \frac{1}{\sqrt{e}} \ll n^{m-1/2} \sum_{1\le k\le n} \tau(|g(k)|) \\
&\ll n^{m+1/2}(\log n)^{c_1+1} = O\left(\frac{n^{m+1}}{\log n}\right).
\end{aligned}$$

So, the last term on the right in (38) is $S_1 + S_2 = O(n^{m+1}/\log n)$. From relation (38), we now get

$$A_2(n) = \frac{C_0' n^{m+1}}{m+1} + O\left(\frac{n^{m+1}}{\log n}\right).$$

We thus get that

$$\log \operatorname{lcm}[u_{a_1},\ldots,u_{a_n}] = \left(\frac{C_0'\log|\alpha_1|}{m+1}\right) n^{m+1} + O\left(\frac{n^{m+1}}{\log n}\right).$$

Since $\alpha_1 = \alpha_0/\sqrt{T_0} = \alpha^C/\sqrt{T_0}$, and

$$\log\left|\prod_{\substack{1\le k\le n \\ a_k\ne 0}} u_{a_k}\right| = \left(\frac{\log|\alpha| C_0}{m+1}\right) n^{m+1} + O\left(\frac{n^{m+1}}{\log n}\right)$$

(see (25)), we get that

$$\frac{\log \left|\prod_{\substack{1\le k\le n\\ a_k\ne 0}} u_{a_k}\right|}{\log \operatorname{lcm}[u_{a_1},\ldots,u_{a_n}]} = \frac{1}{1-\kappa_0} + O\left(\frac{1}{\log n}\right),$$

where

$$\kappa_0 = \frac{\gcd(A_0^2, B_0)}{2\log|\alpha_0|} = \frac{\gcd((u_{2C}/u_C)^2, B^C)}{2\log|\alpha|^C}.$$

It is easy to show using formula (5) that κ_0 does not depend on C so in particular $\kappa_0 = \kappa$. The proof of Theorem 1 is finished.

3.4.2 Proof of Theorem 2

We start with the following lemma.

Lemma 3. *We have $g(X) = (aX+b)^m$ for some coprime integers $a > 0$ and b.*

Proof. We can clearly write $g(X) = (aX+b)^m$ for some complex numbers a and b. Identifying the first two coefficients we get $C_0' = a^m$, $C_1' = ma^{m-1}b$, so $b/a = C_1'/(mC_0') \in \mathbb{Q}$. Further, $a^m = C_0' > 0$, so we may assume, up to replacing (a,b) by $(a\zeta, b\zeta)$, where ζ is some root of order m of unity, that $a = a_1\rho^{1/m}$, where $a_1 > 0$ is an integer and $\rho > 0$ is an integer which is mth power free. Since $b/a \in \mathbb{Q}$ and $b^m = C_m'$, it follows that $b = b_1\rho^{1/m}$ for some integer b_1. Thus, $g(X) = \rho(a_1X+b_1)^m$, so ρ divides all the coefficients of $g(X)$, therefore $\rho = 1$. □

In the instance when $g(X)$ had at least two roots, we found a suitable set of large numbers $d = g(k)/e$ for which $r(d) = 1$ namely all numbers in $\mathcal{D}_n \backslash (\mathcal{D}_{1,n} \cup \mathcal{D}_{2,n})$ except for $\mathcal{D}_{3,n}$. In the present case, we replace this by the following.

Lemma 4. *Every $d = g(k)/e \in \mathcal{D}_n \backslash (\mathcal{D}_{1,n} \cup \mathcal{D}_{2,n})$ can be represented uniquely as $d = g(k)/e$ for some e which is mth power free.*

Proof. This is trivial since if $g(k_1)/e_1 = g(k_2)/e_2$, then, by Lemma 3, we have $e_1/e_2 = ((ak_1+b)/(ak_2+b))^m$, and the number on the left is mth power free, while the number on the right is an mth power. Thus, both are equal to 1, so $e_1 = e_2$ and $k_1 = k_2$. □

We need also the following easy fact about multiplicative functions.

Lemma 5. *We have*

$$n^m \prod_{p|n} \left(1 - \frac{1}{p^m}\right) = \sum_{\substack{e|n^m \\ e \text{ } m\text{th power free}}} \phi(n^m/e).$$

Proof. Both functions above are multiplicative, the one on the left for obvious reasons, while the one on the right because it is the convolution of the multiplicative function $n \mapsto \phi(n^m)$ with the characteristic function of the set of mth power free numbers. If $n = p^\alpha$ for some prime p and integer exponent $\alpha \geq 1$, then the formula becomes

$$\begin{aligned} p^{(\alpha-1)m}(p^m - 1) &= \sum_{f=0}^{m-1} \phi(p^{\alpha m - f}) = \sum_{f=0}^{m-1} (p-1)p^{m\alpha - f - 1} \\ &= (p-1)p^{(\alpha-1)m}(1 + p + \cdots + p^{m-1}) \\ &= (p-1)p^{(\alpha-1)m}\left(\frac{p^m - 1}{p - 1}\right) \\ &= p^{(\alpha-1)m}(p^m - 1), \end{aligned}$$

which is what we wanted. □

We now continue our argument. Instead of relation (36) which leads immediately to (37), we use Lemma 5 to get that the analogous relation (37) in this case is:

$$\begin{aligned} \sum_{\substack{e|ak+b \\ \mu(e)^2=1}} \mu(e) \left(\frac{ak+b}{e}\right)^m &= \sum_{\substack{e|g(k) \\ e<c_3(\log n)^{c_1+1} \\ e \text{ } m\text{th power free}}} \phi\left(\frac{(ak+b)^m}{e}\right) \\ &+ O\left(n^m \sum_{\substack{e|g(k) \\ e>c_3(\log n)^{c_1+1}}} \frac{1}{e}\right). \end{aligned}$$

We now sum up the above relation over all $k \in \mathcal{K}_n$ getting

$$\sum_{k\in\mathcal{K}_n}\sum_{\substack{e\mid ak+b\\ \mu(e)^2=1}}\mu(e)\left(\frac{ak+b}{e}\right)^m = \sum_{k\in\mathcal{K}_n}\sum_{\substack{e\mid g(k)\\ e<c_3(\log n)^{c_1+1}\\ e\ m\text{th power free}}}\phi\left(\frac{(ak+b)^m}{e}\right) + O\left(n^m\sum_{k\in\mathcal{K}_n}\sum_{\substack{e\mid g(k)\\ e>c_3(\log n)^{c_1+1}}}\frac{1}{e}\right). \quad (39)$$

The issue about overcounting elements in $\mathcal{D}_n$ no longer appears by Lemma 4, so the right–hand side in (39) above is equal to $A_2(n)+O(n^{m+1}/\log n)$. Note that if $e \mid ak+b$ for some $k \in \mathcal{K}_n$, then e and a are coprime and $e \le an+b$. We change the order of summation in the left hand side of (39):

$$\begin{aligned}
&\sum_{\substack{1\le e\le an+b\\ (e,a)=1\\ \mu^2(e)=1}}\frac{\mu(e)}{e^m}\sum_{\substack{k\in\mathcal{K}_n\\ ak+b\equiv 0 \pmod e}}(a^mk^m+O(n^{m-1}))\\
=\ & a^m\sum_{\substack{1\le e\le an+b\\ \mu^2(e)=1}}\frac{\mu(e)}{e^m}\sum_{\substack{k\in\mathcal{K}_n\\ ak+b\equiv 0 \pmod e}}k^m+O\left(n^{m-1}\#\mathcal{K}_n\sum_{e\le an+b}\frac{1}{e}\right)\\
=\ & a^m\sum_{\substack{1\le e\le an+b\\ (e,a)=1\\ \mu^2(e)=1}}\frac{\mu(e)}{e^m}\left(\sum_{\substack{1\le k\le n\\ ak+b\equiv 0 \pmod e}}k^m-\sum_{\substack{1\le k\le n/(\log n)^{c_1+1}\\ ak+b\equiv 0 \pmod e}}k^m\right)\\
+\ & O(n^m\log n)\\
=\ & a^m\sum_{\substack{1\le e\le an+b\\ (e,a)=1\\ \mu^2(e)=1}}\frac{\mu(e)}{e^m}\sum_{\substack{1\le k\le n\\ ak+b\equiv 0 \pmod e}}k^m+O(n^m\log n)\\
+\ & O\left(\frac{n^{m+1}}{(\log n)^{(m+1)(c_1+1)}}\sum_{e\le an+|b|}\frac{1}{e}\right)\\
=\ & a^m\sum_{\substack{1\le e\le an+b\\ (e,a)=1\\ \mu^2(e)=1}}\frac{\mu(e)}{e^m}\sum_{\substack{1\le k\le n\\ ak+b\equiv 0 \pmod e}}k^m+O\left(\frac{n^{m+1}}{\log n}\right). \qquad (40)
\end{aligned}$$

For the inner sum, we use Abel's summation formula together with the fact that the counting function of the set of $k \le n$ such that $ak+b \equiv 0 \pmod e$ is $n/e + O(1)$. We get

$$\begin{aligned}
\sum_{\substack{1\le k\le n\\ ak+b\equiv 0 \pmod e}} k^m &= \left(\frac{n}{e}+O(1)\right)n^m - m\int_1^n \left(\frac{t}{e}+O(1)\right)t^{m-1}dt \\
&= \frac{n^{m+1}}{e} + O(n^m) - m\int_1^n \frac{t^m}{e}dt + O\left(\int_1^n t^{m-1}dt\right) \\
&= \frac{n^{m+1}}{e} - \left(\frac{mt^{m+1}}{m+1}\Big|_{t=1}^{t=n}\right) + O(n^m) \\
&= \frac{n^{m+1}}{(m+1)e} + O(n^m).
\end{aligned}$$

Inserting this into (40), we get

$$\begin{aligned}
A_2(n) &= a^m \sum_{\substack{1\le e\le an+b\\ (e,a)=1\\ \mu^2(e)=1}} \frac{\mu(e)}{e^m}\left(\frac{n^{m+1}}{(m+1)e}+O(n^m)\right) + O\left(\frac{n^{m+1}}{\log n}\right) \\
&= \frac{a^m n^{m+1}}{(m+1)} \sum_{\substack{1\le e\le an+b\\ (e,a)=1\\ \mu^2(e)=1}} \frac{\mu(e)}{e^{m+1}} + O\left(n^m \sum_{e\le an+b}\frac{1}{e} + \frac{n^{m+1}}{\log n}\right) \\
&= \frac{a^m n^{m+1}}{(m+1)}\left(\sum_{\substack{e\ge 1\\ (e,a)=1\\ \mu^2(e)=1}} \frac{\mu(e)}{e^{m+1}} - \sum_{\substack{e> an+b\\ (e,a)=1\\ \mu^2(e)=1}} \frac{\mu(e)}{e^{m+1}}\right) + O\left(\frac{n^{m+1}}{\log n}\right) \\
&= \frac{a^m n^{m+1}}{(m+1)} \prod_{p\nmid a}\left(1-\frac{1}{p^{m+1}}\right) + O\left(n^{m+1}\sum_{e>an+b}\frac{1}{e^2} + \frac{n^{m+1}}{\log n}\right) \\
&= \left(\frac{a^m \zeta(m+1)^{-1}}{(m+1)} \prod_{p|a}\left(1-\frac{1}{p^{m+1}}\right)^{-1}\right) n^{m+1} + O\left(\frac{n^{m+1}}{\log n}\right) \\
&= \left(\frac{C_0'\zeta(m+1)^{-1}}{(m+1)} \prod_{p|a}\left(1-\frac{1}{p^{m+1}}\right)^{-1}\right) n^{m+1} + O\left(\frac{n^{m+1}}{\log n}\right).
\end{aligned}$$

So, we get to the conclusion that

$$\log|\prod_{\substack{1\le k\le n\\ a_k\neq 0}} u_{a_k}| = \left(\frac{\log|\alpha|C_0}{m+1}\right) n^{m+1} + O\left(\frac{n^{m+1}}{\log n}\right)$$

while

$$\begin{aligned}\log \operatorname{lcm}[u_{a_1},\ldots,u_{a_n}] \quad &= \quad \left(\frac{\log|\alpha_1|C_0'}{(m+1)\zeta(m+1)}\prod_{p|a}\left(1-\frac{1}{p^{m+1}}\right)^{-1}\right) n^{m+1}\\ &+ \quad O\left(\frac{n^{m+1}}{\log n}\right),\end{aligned}$$

This leads to

$$\frac{\log\left|\prod_{\substack{1\le k\le n\\ a_k\neq 0}} u_{a_k}\right|}{\log \operatorname{lcm}[u_{a_1},\ldots,u_{a_n}]} = \frac{\zeta(m+1)}{1-\kappa}\prod_{p|a}\left(1-\frac{1}{p^{m+1}}\right) + O\left(\frac{1}{\log n}\right).$$

Thus, we obtained Theorem 2.

Acknowledgments. We thank the referee for comments which improved the quality of this paper. S. A. is supported by the Japanese Society for the Promotion of Science (JSPS), grant in aid 21540010. F. L. worked on this project during a visit to Niigata University in January 2012 with a JSPS Fellowship. This author thanks JSPS for support and Niigata University for its hospitality. He was also supported in part by Project PAPIIT IN104512, CONACyT 163787, CONACyT 193539 and a Marcos Moshinsky Fellowship.

References

[1] S. Akiyama, "Lehmer numbers and an asymptotic formula for π", *J. Number Theory* **39** (1990), 328–331.

[2] S. Akiyama, "A new type of inclusion exclusion principle for sequences and asymptotic formulas for π", *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", *Japanese J. Math.* **22** (1996), 129–146.

[4] Yu. Bilu, G. Hanrot, and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine Angew. Math. **539** (2001), 75–122, With an appendix by M. Mignotte.

[5] P. Erdős, "On the normal number of prime factors of $p-1$ and some related problems concerning Euler's ϕ function", *Quart. J. Math. Oxford* **6** (1935), 205–213.

[6] A. Flatters, *Primitive divisors of some Lehmer-Pierce sequences*, J. Number Theory **129** (2009), 209–219.

[7] K. Ford, "The distribution of totients", *The Ramanujan Journal* **2** (1998), 67–151.

[8] G. Everest, G. Mclaren, and T. Ward, *Primitive divisors of elliptic divisibility sequences*, J. Number Theory **118** (2006), 71–89.

[9] Graham Everest and Thomas Ward, *Primes in divisibility sequences*, Cubo Mat. Educ. **3** (2001), 245–259.

[10] P. Ingram, *Elliptic divisibility sequences over certain curves*, J. Number Theory **123** (2007), 473–486.

[11] P. Ingram and J. H. Silverman, *Uniform estimates for primitive divisors in elliptic divisibility sequences*, Number Theory, Analysis and Geometry, 2012, 243–271.

[12] J. P. Jones and P. Kiss, *An asymptotic formula concerning Lehmer numbers*, *Publ. Math. Debrecen* **42** (1993), 199—13.

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

[14] F. Luca, *Arithmetic properties of members of a binary recurrent sequence*, Acta Arith. **109** (2003), 81–107.

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

[16] T. Nagell, *Introduction to Number Theory*, New York, Wiley, 1951.

[17] A. Schinzel, *Second order strong divisibility sequences in an algebraic number field*, Arch. Math. (Brno) **23** (1987), 181–186.

[18] H. N. Shapiro, *Introduction to the theory of numbers*, John Wiley and Sons, 1983.

[19] C. L. Stewart, "On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers", *Proc. London Math. Soc.* **35** (1977), 425–447.

[20] J. G. van der Corput, "Une inégalité relative au nombre des diviseurs", *Indag. Math.* **1** (1939), 177–183.

[21] R. T. Worley, "Estimating $|\alpha - p/q|$", *J. Australian Math. Soc. (Series A)* **31** (1981), 202–206.

[22] M. Yabuta, *Primitive divisors of certain elliptic divisibility sequences*, Experiment. Math. **18** (2009), 303–310.