On numbers n dividing the nth term of a Lucas sequence

Published version:

DOI:10.1142/S1793042117500373

(Article begins on next page)

International Journal of Number Theory

ON NUMBERS n DIVIDING THE n-TH TERM OF A LUCAS SEQUENCE

CARLO SANNA

Department of Mathematics
Università degli Studi di Torino
Via Carlo Alberto 10, 10123 Torino, Italy
carlo.sanna.dev@gmail.com

Received (Day Month Year)
Accepted (Day Month Year)

We prove that if $(u_n)_{n\geq 0}$ is a Lucas sequence satisfying some mild hypotheses, then the number of positive integers n not exceeding x and such that n divides u_n is less than

$$x^{1-(1/2+o(1))\log\log\log x/\log\log x},$$

as $x \to \infty$. This both generalizes a result of Luca and Tron about the positive integers n dividing the n-th Fibonacci number, and improves a previous upper bound due to Alba González, Luca, Pomerance, and Shparlinski.

Keywords: Lucas sequence; divisibility; rank of apparition; p-adic valuation.

Mathematics Subject Classification 2010: 11B37, 11B39, 11A07, 11N25

1. Introduction

Let $(u_n)_{n\geq 0}$ be a Lucas sequence, that is, a sequence of integers such that $u_0 = 0$, $u_1 = 1$, and $u_n = au_{n-1} + bu_{n-2}$ for any $n \geq 2$, where a and b are two relatively prime integers.

In the early '90s, André-Jeannin [2] and Somer [8] initiated a systematic study of the positive integers n such that u_n is divisible by n. For this purpose, we will see that there is no loss of generality in assuming that $(u_n)_{n\geq 0}$ is nondegenerate, i.e., $b \neq 0$ and the ratio α/β of the two roots $\alpha, \beta \in \mathbb{C}$ of the characteristic polynomial $f(X) := X^2 - aX - b$ is not a root of unity; and that the discriminant of $f(X)$ is not equal to 1. Under those assumptions, the set $\mathcal{A} := \{n \geq 1 : n \mid u_n\}$ is infinite, so it is interesting to study the distribution of its elements among the positive integers. Put $\mathcal{A}(x) := \mathcal{A} \cap [1, x]$ and $A(x) := \#\mathcal{A}(x)$, for each $x \geq 1$.

Alba González, Luca, Pomerance, and Shparlinski [1] proved the following upper and lower bounds for $A(x)$.

Theorem 1.1. *It holds*

$$\exp(C(\log\log x)^2) \leq A(x) \leq \frac{x}{\exp((1+o(1))\sqrt{\log x \log\log x})},$$

as $x \to \infty$, where $C > 0$ is a constant depending on a and b.

Luca and Tron [4] showed that if $(u_n)_{n \geq 0}$ is the sequence of Fibonacci numbers, then the upper bound of Theorem 1.1 can be improved considerably. Indeed, they claimed that their methods should apply equally well to other Lucas sequences.

In this paper, using the ideas of Luca and Tron together with some results of the author concerning the p-adic valuation of Lucas sequences, we prove the following upper bound.

Theorem 1.2. *It holds*

$$\log A(x) \leq \log x - \left(\frac{1}{2} + o(1)\right) \frac{\log x \log\log\log x}{\log\log x},$$

as $x \to \infty$, where the $o(1)$ depends on a and b.

Notation

For any prime number p, we write $\nu_p(\cdot)$ for the usual p-adic valuation over the integers. Moreover, for integers v and n, we write $p^v \mid\mid n$ to mean that $\nu_p(n) = v$.

2. Preliminaries

First of all, we have to justify our claim that in order to study $\mathcal{A}$ there is no loss of generality in assuming that $(u_n)_{n \geq 0}$ is nondegenerate and that the discriminant $\Delta := a^2 + 4b$ of the characteristic polynomial $f(X)$ satisfies $\Delta \neq 1$.

On the one hand, if $(u_n)_{n \geq 0}$ is a degenerate Lucas sequence, then it is known [6, pp. 5–6] that $(a, b) \in \{(\pm 2, -1), (\pm 1, -1), (0, \pm 1), (\pm 1, 0)\}$ and in each of such cases $(u_n)_{n \geq 0}$ is either definitely periodic with values in $\{0, -1, +1\}$, or equal to $(n)_{n \geq 0}$, or equal to $((-1)^{n-1} n)_{n \geq 0}$, so determining $\mathcal{A}$ is trivial. On the other hand, if $\Delta = 1$ then by [8, Theorem 8(iii)] it follows that $\mathcal{A} = \{1\}$, another trivial case.

Now we recall that for each positive integer m relatively prime with b,

$$\tau(m) := \min\{n \geq 1 : m \mid u_n\}$$

is well-defined and called the *rank of apparition* of m in $(u_n)_{n \geq 0}$. The following lemmas state some of the most important properties of the rank of apparition (see, e.g., [5]).

Lemma 2.1. *For each integer $m \geq 1$, we have $m \mid u_n$ for some positive integer n if and only if $\gcd(m, b) = 1$ and $\tau(m) \mid n$.*

Lemma 2.2. *Let $m, n \geq 1$ be integers such that $\gcd(b, mn) = 1$, then:*

(1) If $m \mid n$ then $\tau(m) \mid \tau(n)$.
(2) $\tau(\mathrm{lcm}(m, n)) = \mathrm{lcm}(\tau(m), \tau(n))$.
(3) $\tau(m) = \mathrm{lcm}\{\tau(p^v) : p^v \mid\mid m\}$, where p runs over all the prime factors of m.

Lemma 2.3. *Let p be a prime number not dividing b. Then $\tau(p) \mid p - (-1)^{p-1}\big(\frac{\Delta}{p}\big)$, where $\big(\frac{\cdot}{p}\big)$ is the Legendre symbol. In particular, $\tau(p) = p$ if and only if $p \mid \tau(p)$ if and only if $p \mid \Delta$.*

Note that, assuming $(u_n)_{n\geq 0}$ nondegenerate, we have $u_n \neq 0$ for all positive integers n, hence $\nu_p(u_n)$ is finite for any prime number p.

Sanna [7] proved the following formulas for the p-adic valuation of nondegenerate Lucas sequences.

Theorem 2.4. *If p is a prime number such that $p \nmid b$, then*

$$\nu_p(u_n) = \begin{cases} \nu_p(n) + \nu_p(u_p) - 1 & \text{if } p \mid \Delta,\ p \mid n, \\ 0 & \text{if } p \mid \Delta,\ p \nmid n, \\ \nu_p(n) + \nu_p(u_{p\tau(p)}) - 1 & \text{if } p \nmid \Delta,\ \tau(p) \mid n,\ p \mid n, \\ \nu_p(u_{\tau(p)}) & \text{if } p \nmid \Delta,\ \tau(p) \mid n,\ p \nmid n, \\ 0 & \text{if } p \nmid \Delta,\ \tau(p) \nmid n, \end{cases}$$

for each positive integer n. Moreover, if $p \geq 3$ then

$$\nu_p(u_n) = \begin{cases} \nu_p(n) + \nu_p(u_p) - 1 & \text{if } p \mid \Delta \text{ and } p \mid n, \\ 0 & \text{if } p \mid \Delta \text{ and } p \nmid n, \\ \nu_p(n) + \nu_p(u_{\tau(p)}) & \text{if } p \nmid \Delta \text{ and } \tau(p) \mid n, \\ 0 & \text{if } p \nmid \Delta \text{ and } \tau(p) \nmid n, \end{cases}$$

for each positive integer n.

Now we prove some formulas for the rank of apparition of the power of a prime number.

Lemma 2.5. *Let p be a prime number such that $p \nmid b$, and let v be a positive integer. Then*

$$\tau(p^v) = \begin{cases} \tau(p) & \text{if } v \leq \nu_p(u_{\tau(p)}), \\ p^{\max\{1,\, v - \nu_p(u_{p\tau(p)}) + 1\}}\, \tau(p) & \text{if } v > \nu_p(u_{\tau(p)}) \text{ and } p = 2 \nmid \Delta, \\ p^{v - \nu_p(u_{\tau(p)})}\, \tau(p) & \text{otherwise.} \end{cases}$$

Proof. Since $p^v \mid u_{\tau(p^v)}$, clearly $p \mid u_{\tau(p^v)}$, so it follows from Lemma 2.1 that $\tau(p) \mid \tau(p^v)$. We write $\tau(p^v) = m\tau(p)$, for some positive integer m. Suppose that there exists a prime number $q \neq p$ such that $q \mid m$. Then, from Theorem 2.4 it follows easily that $\nu_p(u_{\tau(p^v)/q}) = \nu_p(u_{\tau(p^v)})$, and thus $p^v \mid u_{\tau(p^v)/q}$, absurd. Hence $m = p^r$, for some nonnegative integer r, and $\tau(p^v) = p^r\tau(p)$. Precisely, r is the least nonnegative integer such that $\nu_p(u_{p^r\tau(p)}) \geq v$. If $v \leq \nu_p(u_{\tau(p)})$, then obviously $r = 0$ and $\tau(p^v) = \tau(p)$. Suppose $v > \nu_p(u_{\tau(p)})$, so that, clearly, $r \geq 1$.

On the one hand, if $p = 2$ and Δ is odd, then thanks to Lemma 2.3 we have $p \nmid \tau(p)$, and from Theorem 2.4 it follows that

$$\nu_p(u_{p^s\tau(p)}) = \nu_p(p^s\tau(p)) + \nu_p(u_{p\tau(p)}) - 1 = s + \nu_p(u_{p\tau(p)}) - 1,$$

for each positive integer s, hence $r = \max\{1,\, v - \nu_p(u_{p\tau(p)}) + 1\}$.

On the other hand, if $p \mid \Delta$ or $p \geq 3$, then using Lemma 2.3 and Theorem 2.4 one can easily check that $\nu_p(u_{p^s\tau(p)}) = s + \nu_p(u_{\tau(p)})$, for each positive integer s, hence $r = v - \nu_p(u_{\tau(p)})$. □

We state a last lemma regarding the p-adic valuation of Lucas sequence [7, Lemma 3.2].

Lemma 2.6. *If p is a prime number such that $p \nmid b$, then*

$$\nu_p(u_{p\tau(p)}) \geq \nu_p(u_{\tau(p)}) + 1,$$

with equality if $p \geq 5$, or if $p = 3$ and $3 \nmid \Delta$.

3. Proof of Theorem 1.2

For each positive integer k, put $\mathcal{A}_k := \{n \in \mathcal{A} : n = k \cdot \tau(n)\}$. Clearly, $(\mathcal{A}_k)_{k \geq 1}$ is a partition of $\mathcal{A}$. In this section, we shall give a description of the elements of each nonempty $\mathcal{A}_k$ in terms of k and a function $\gamma(k)$. This will be the key ingredient in the proof of Theorem 1.2. For each integer $i \geq 0$, we write τ^i for the i-th iteration of the rank of apparition, with the usual convention that τ^0 is the identity function. Note that since $\tau(m)$ is defined only for the positive integers m relatively prime with b, we have that $\tau^{i+1}(m)$ is defined if and only if $m, \tau(m), \ldots, \tau^i(m)$ are all relatively prime with b.

Lemma 3.1. *Suppose that k is a positive integer such that $\mathcal{A}_k \neq \varnothing$. Then*

$$\gamma(k) := k \cdot \operatorname{lcm}\{\tau^i(k) : i \geq 1\}$$

is well-defined. Moreover, $\gamma(k) \mid n$ for each $n \in \mathcal{A}_k$.

Proof. In order to prove that $\gamma(k)$ is well-defined, we need to show two things. First, that each iterate $\tau^i(k)$ is defined. Second, that the set $\{\tau^i(k) : i \geq 1\}$ is finite, so that it makes sense to take the least common multiple of its elements. Since $\mathcal{A}_k$ is nonempty, pick $n \in \mathcal{A}_k$. We shall prove that

$$\gamma_i := k \cdot \operatorname{lcm}\{\tau(k), \tau^2(k), \ldots, \tau^i(k), \tau^{i+1}(n)\} \mid n, \qquad (3.1)$$

for each integer $i \geq 0$, showing in the course of the proof that all the iterates of τ in (3.1) are defined. We proceed by induction on i. For $i = 0$, the claim is obvious, since $\gamma_0 := k \cdot \operatorname{lcm}\{\tau(n)\} = k \cdot \tau(n) = n$. Suppose that (3.1) holds for $i \geq 0$, we will prove it for $i + 1$. Since $n \in \mathcal{A}$, by Lemma 2.1 we have $\gcd(n, b) = 1$, so that from (3.1) it follows that $\tau(k), \tau^2(k), \ldots, \tau^i(k), \tau^{i+1}(n)$ are all relatively prime with b, hence $\tau^{i+2}(n)$ and γ_{i+1} are well-defined. From Lemma 2.2 and using the induction hypothesis, we obtain

$$\begin{aligned}\gamma_{i+1} &= k \cdot \operatorname{lcm}\{\tau(k), \tau^2(k), \ldots, \tau^{i+1}(k), \tau^{i+2}(n)\} \\ &= k \cdot \tau(\operatorname{lcm}\{k, \tau(k), \ldots, \tau^i(k), \tau^{i+1}(n)\}) \\ &\mid\ k \cdot \tau(k \cdot \operatorname{lcm}\{\tau(k), \ldots, \tau^i(k), \tau^{i+1}(n)\}) \\ &= k \cdot \tau(\gamma_i) \\ &\mid\ k \cdot \tau(n) = n,\end{aligned}$$

since $n \in \mathcal{A}_k$, hence the claim is proved. Therefore, each iterate $\tau^i(k)$ is defined. Moreover, from (3.1) if follows that $\tau^i(k) \leq n$ for each integer $i \geq 1$, so that the set $\{\tau^i(k) : i \geq 1\}$ is finite. Thus we have proved that $\gamma(k)$ is well-defined. Finally, since $\{\tau^i(k) : i \geq 1\}$ is finite, for any sufficiently large i we have $\gamma(k) \mid \gamma_i \mid n$. But n is arbitrary, hence $\gamma(k) \mid n$ for each $n \in \mathcal{A}_k$. □

The next lemma shows that, actually, $\gamma(k)$ is the least element of $\mathcal{A}_k$.

Lemma 3.2. *Suppose that k is a positive integer such that $\mathcal{A}_k \neq \varnothing$. Then*

$$\gamma(k) = \min(\mathcal{A}_k) = \gcd(\mathcal{A}_k).$$

Proof. Since from Lemma 3.1 we know that $\gamma(k) \mid n$ for any $n \in \mathcal{A}_k$, it is sufficient to prove that $\gamma(k) \in \mathcal{A}_k$, i.e., that $\gamma(k) = k \cdot \tau(\gamma(k))$. From Lemma 2.2 we have

$$\begin{aligned}\gamma(k) &= k \cdot \operatorname{lcm}\{\tau^i(k) : i \geq 1\} = k \cdot \tau(\operatorname{lcm}\{\tau^i(k) : i \geq 0\}) \\ &\mid\ k \cdot \tau(k \cdot \operatorname{lcm}\{\tau^i(k) : i \geq 1\}) = k \cdot \tau(\gamma(k)),\end{aligned}$$

so it remains to prove that $k \cdot \tau(\gamma(k)) \mid \gamma(k)$. For the rest of the proof, we reserve the letters p and q for prime numbers. Using Lemma 2.2, one can easily prove by induction that $\tau^i(k) = \operatorname{lcm}\{\tau^i(p^v) : p^v \mid\mid k\}$, for each integer $i \geq 1$. Therefore,

$$\begin{aligned}\gamma(k) &= k \cdot \operatorname{lcm}\{\tau^i(k) : i \geq 1\} \\ &= k \cdot \operatorname{lcm}\{\operatorname{lcm}\{\tau^i(p^v) : p^v \mid\mid k\} : i \geq 1\} \\ &= k \cdot \operatorname{lcm}\{\tau^i(p^v) : i \geq 1,\ p^v \mid\mid k\}.\end{aligned} \tag{3.2}$$

If for each prime number q we set

$$m_q := \nu_q(\operatorname{lcm}\{\tau^i(p^v) : i \geq 1,\ p^v \mid\mid k\}) = \max\{\nu_q(\tau^i(p^v)) : i \geq 1,\ p^v \mid\mid k\},$$

then from (3.2) it follows that

$$\gamma(k) = \operatorname{lcm}\Big(\Big\{\prod_{p^v \mid\mid k} p^{v+m_p}\Big\} \cup \{\tau^i(p^v) : i \geq 1,\ p^v \mid\mid k\}\Big).$$

Thus Lemma 2.2 yields

$$\begin{aligned}\tau(\gamma(k)) &= \operatorname{lcm}\Big(\Big\{\tau\Big(\prod_{p^v \mid\mid k} p^{v+m_p}\Big)\Big\} \cup \{\tau^{i+1}(p^v) : i \geq 1,\ p^v \mid\mid k\}\Big) \\ &= \operatorname{lcm}\Big(\{\operatorname{lcm}\{\tau(p^{v+m_p}) : p^v \mid\mid k\}\} \cup \{\tau^{i+1}(p^v) : i \geq 1,\ p^v \mid\mid k\}\Big) \\ &= \operatorname{lcm}\Big(\{\tau(p^{v+m_p}) : p^v \mid\mid k\} \cup \{\tau^{i+1}(p^v) : i \geq 1,\ p^v \mid\mid k\}\Big).\end{aligned} \tag{3.3}$$

At this point, it is sufficient to prove that $\nu_q(\tau(p^{v+m_p})) \leq m_q$ for any prime numbers p and q with $p^v \parallel k$. In fact, this last claim together with (3.3) and (3.2) implies that

$$\nu_q(k \cdot \tau(\gamma(k))) \leq \nu_q(k) + m_q = \nu_q(\gamma(k)),$$

for each prime number q, i.e., $k \cdot \tau(\gamma(k)) \mid \gamma(k)$.

If $m_q = 0$, then the claim is obvious, since $\nu_q(\tau(p^{v+m_p})) = \nu_q(\tau(p^v)) \leq m_q$, by the definition of m_q. Thus, we assume $m_q \geq 1$. If $q \neq p$, then from Lemma 2.5 we get immediately that $\nu_q(\tau(p^{v+m_p})) = \nu_q(\tau(p^v)) \leq m_q$, again by the definition of m_q. Hence, we suppose $q = p$. Since $\mathcal{A}_k$ is nonempty, pick $n \in \mathcal{A}_k$, so that $n = k \cdot \tau(n)$. We can write $k = p^v k'$ and $n = p^v n'$, where k' and n' are positive integers, with $p \nmid k'$. Therefore, since $n \mid u_{\tau(n)}$,

$$v + \nu_p(n') = \nu_p(n) \leq \nu_p(u_{\tau(n)}) = \nu_p(u_{n'/k'}). \tag{3.4}$$

Using Theorem 2.4 and the fact that $p \nmid k'$, we can compute $\nu_p(u_{n'/k'})$ and from (3.4) we obtain

$$v \leq \begin{cases} \nu_p(u_p) - 1 & \text{if } p \mid \Delta, \\ \nu_p(u_{p\tau(p)}) - 1 & \text{if } p \nmid \Delta \text{ and } p \mid n', \\ \nu_p(u_{\tau(p)}) & \text{if } p \nmid \Delta \text{ and } p \nmid n'. \end{cases} \tag{3.5}$$

Now from Lemma 2.5 we get that: If $v + m_p \leq \nu_p(u_{\tau(p)})$, then

$$\nu_p(\tau(p^{v+m_p})) = \nu_p(\tau(p)) = \nu_p(\tau(p^v)) \leq m_p;$$

If $v + m_p > \nu_p(u_{\tau(p)})$ and $p = 2 \nmid \Delta$, then

$$\begin{aligned} \nu_p(\tau(p^{v+m_p})) &= \max\{1, v + m_p - \nu_p(u_{p\tau(p)}) + 1\} + \nu_p(\tau(p)) \\ &\leq \max\{1, m_p\} = m_p, \end{aligned}$$

where we have used inequality (3.5), Lemma 2.6, and the fact that $p \nmid \tau(p)$, in the light of $p \nmid \Delta$ and Lemma 2.3.

Otherwise, if $v + m_p > \nu_p(u_{\tau(p)})$ and it is not the case that $p = 2 \nmid \Delta$, then

$$\nu_p(\tau(p^{v+m_p})) = v + m_p - \nu_p(u_{\tau(p)}) + \nu_p(\tau(p)).$$

Consider this last case. If $p \mid \Delta$ then $\tau(p) = p$, by Lemma 2.3, and from (3.5) we obtain

$$\nu_p(\tau(p^{v+m_p})) \leq \nu_p(u_p) - 1 + m_p - \nu_p(u_p) + \nu_p(p) = m_p.$$

Therefore, assume $p \nmid \Delta$, so again by Lemma 2.3 we have $p \nmid \tau(p)$. If $p \mid n'$ then by (3.5), and since in Lemma 2.6 equality holds, we have

$$\nu_p(\tau(p^{v+m_p})) \leq \nu_p(u_{p\tau(p)}) - 1 + m_p - \nu_p(u_{\tau(p)}) + \nu_p(\tau(p)) = m_p.$$

Finally, if $p \nmid n'$ then by (3.5) we have

$$\nu_p(\tau(p^{v+m_p})) \leq \nu_p(u_{\tau(p)}) + m_p - \nu_p(u_{\tau(p)}) + \nu_p(\tau(p)) = m_p.$$

In conclusion, $\nu_p(\tau(p^{v+m_p})) \leq m_p$ as claimed and the proof is complete. □

Now we are ready to state the characterization of the elements of $\mathcal{A}_k$ in terms of k and $\gamma(k)$.

Lemma 3.3. *Suppose that k and n are positive integers such that $n \in \mathcal{A}_k$. Then $n = \gamma(k)m$, where m is some positive integer such that each of its prime factors divides $6\Delta k$.*

Proof. From Lemma 3.1 we already know that $\gamma(k) \mid n$, i.e., $n = \gamma(k)m$ for some positive integer m. For the sake of contradiction, suppose that m has a prime factor p such that $p \nmid 6\Delta k$. Actually, we can suppose that p is the greatest among such prime factors. Since $n \in \mathcal{A}_k$, by Lemma 2.2 we have

$$n = k \cdot \tau(n) = k \cdot \operatorname{lcm}\{\tau(q^v) : q^v \mid\mid n\},$$

where, henceforth, the variable q is reserved for prime numbers. Thus, since $p \nmid k$, we have

$$\nu_p(n) = \max\{\nu_p(\tau(q^v)) : q^v \mid\mid n\}. \tag{3.6}$$

Note that $p \nmid \Delta$ implies $\nu_p(\tau(p)) = 0$, thanks to Lemma 2.3. Now by Lemma 2.5 we have that: On the one hand, since $p \neq 2$, it holds

$$\nu_p(\tau(p^{\nu_p(n)})) = \max\{\nu_p(n) - \nu_p(u_{\tau(p)}), 0\} < \nu_p(n);$$

On the other hand, for each prime number $q \neq p$ and each positive integer v, it holds $\nu_p(\tau(q^v)) = \nu_p(\tau(q))$. Therefore, we can simplify (3.6) to

$$\nu_p(n) = \max\{\nu_p(\tau(q)) : q \mid n,\ q \neq p\}. \tag{3.7}$$

From Lemma 3.2 we know that $\gamma(k) \in \mathcal{A}_k$, hence setting $n = \gamma(k)$ in (3.7) we have

$$\nu_p(\gamma(k)) = \max\{\nu_p(\tau(q)) : q \mid \gamma(k),\ q \neq p\}. \tag{3.8}$$

Now subtracting (3.8) from (3.7) and using $n = \gamma(k)m$, we get

$$\begin{aligned}
\max\{\nu_p(\tau(q)) &: q \mid \gamma(k)m,\ q \neq p\} - \max\{\nu_p(\tau(q)) : q \mid \gamma(k),\ q \neq p\} \\
&= \nu_p(\gamma(k)m) - \nu_p(\gamma(k)) \\
&= \nu_p(m) > 0,
\end{aligned}$$

hence there exists a prime number $q \neq p$ such that $q \mid m$, $q \nmid \gamma(k)$ and $\nu_p(\tau(q)) > 0$.

If $q \mid \Delta$, then $\tau(q) = q$ by Lemma 2.3, hence $q = p$, absurd. Thus $q \nmid \Delta$, so that

$$p \mid \tau(q) \mid q \pm 1,$$

again by Lemma 2.3. This together with $p \neq 2, 3$ implies $q > p \geq 5$, and in particular $q \nmid 6$. Furthermore, if $q \mid k$ then $q \mid \gamma(k)$, absurd. In conclusion, $q > p$, $q \mid m$ and $q \nmid 6\Delta k$, but this is absurd by the maximality of p. The proof is complete. □

At this point, the proof of Theorem 1.2 proceeds almost exactly as in the paper of Luca and Tron, with only a few changes. However, we include it here just for completeness.

Let $x > 0$ be sufficiently large and $n \in \mathcal{A}(x)$. Thanks to Lemma 3.3, we know that $n = \gamma(k)m$, for some positive integers k and m, where every prime factor of m divides $6\Delta k$. Put for convenience $C(x) := x^{\log\log\log x/\log\log x}$, and split $\mathcal{A}(x)$ into two disjoint subsets: $\mathcal{A}_1(x)$, the subset of those n such that $k \leq x/C(x)$; and $\mathcal{A}_2(x)$, the subset of the remaining n such that $x/C(x) < k \leq x$.

First, suppose $n \in \mathcal{A}_1(x)$. Let p_s be the s-th prime number, and for each $x \geq y \geq 2$ let $\Psi(x, y)$ denotes the number of positive integers not exceeding x whose largest prime factor is less than or equal to y. Clearly, m has at most $s := \omega(6\Delta k)$ distinct prime factors. Since $k \leq x$ and $\omega(n) \leq (1+o(1)) \log n/\log\log n$, as $n \to \infty$, (see, e.g, [9, §5.3, Theorem 3]) we get that $s \leq 2\log x/\log\log x$, for sufficiently large x, depending on Δ. Therefore, from the Prime Number Theorem it follows that $p_s \leq 5\log x$, for x large enough. Thus, the number of positive integers $m \leq x$ all of whose prime factors divide $6\Delta k$ is at most $\Psi(x, p_s) \leq \Psi(x, 5\log x)$. Putting $y = 5\log x$ in the classical estimate for $\Psi(x, y)$ due to de Bruijn [9, §5.1, Theorem 2], after some computations, we obtain that

$$\Psi(x, 5\log x) \leq x^{\frac{6\log 6 - 5\log 5 + o(1)}{\log\log x}} = C(x)^{o(1)},$$

as $x \to \infty$. Summarizing, for any fixed $k \leq x/C(x)$ there are at most $C(x)^{o(1)}$ values of m.

In conclusion, we have

$$\#\mathcal{A}_1(x) \leq C(x)^{o(1)} \cdot \frac{x}{C(x)} = \frac{x}{C(x)^{1+o(1)}}. \tag{3.9}$$

Now suppose $n \in \mathcal{A}_2(x)$, so that $k > x/C(x)$. By Lemma 3.1, we have $\gamma(k) \geq k\tau(k)$, thus

$$\frac{x}{C(x)}\tau(k) < k\tau(k) \leq \gamma(k) \leq \gamma(k)m = n \leq x,$$

and hence $\tau(k) \leq C(x)$. For any positive integer $\tau \leq C(x)$, put

$$\mathcal{B}_\tau := \{h \geq 1 : \tau(h) = \tau\}$$

and $\mathcal{B}_\tau(y) := \mathcal{B}_\tau \cap [1, y]$, for any $y \geq 1$. Thanks to [3, Theorem 3], we know that

$$\#\mathcal{B}_\tau(y) \leq \frac{y}{C(y)^{1/2+o(1)}},$$

as $y \to \infty$, uniformly in τ. Since $n = \gamma(k)m$ by Lemma 3.1, it follows that n is a multiple of $k\tau(k)$. Clearly, there are at most $x/(k\tau(k))$ multiples of $k\tau(k)$ not exceeding x. Therefore, for any fixed positive integer $\tau \leq C(x)$, the number of

$n \in \mathcal{A}_2(x)$ such that $\tau(k) = \tau$ is at most

$$\begin{aligned}
\sum_{\substack{k \in \mathcal{B}_\tau \\ x/C(x) < k \le x}} \frac{x}{\tau k} &= \frac{x}{\tau} \int_{x/C(x)}^{x} \frac{\mathrm{d}\#\mathcal{B}_\tau(t)}{t} \\
&= \frac{x}{\tau} \left(\frac{\#\mathcal{B}_\tau(t)}{t} \bigg|_{t=x/C(x)}^{x} + \int_{x/C(x)}^{x} \frac{\#\mathcal{B}_\tau(t)}{t^2} \mathrm{d}t \right) \\
&\le \frac{x}{\tau} \left(\frac{\#\mathcal{B}_\tau(x)}{x} + \int_{x/C(x)}^{x} \frac{\mathrm{d}t}{t\, C(t)^{1/2+o(1)}} \right) \\
&\le \frac{x}{\tau} \left(\frac{1}{C(x)^{1/2+o(1)}} + \frac{1}{C(x)^{1/2+o(1)}} \int_{x/C(x)}^{x} \frac{\mathrm{d}t}{t} \right) \\
&= \frac{x(1 + \log C(x))}{\tau\, C(x)^{1/2+o(1)}} = \frac{x}{\tau\, C(x)^{1/2+o(1)}},
\end{aligned}$$

where we used partial summation and the fact that $C(t)^{1/2+o(1)} = C(x)^{1/2+o(1)}$, as $x \to \infty$, uniformly for $t \in [x/C(x), x]$. Summing over all the positive integers $\tau \le C(x)$, we obtain

$$\#\mathcal{A}_2(x) \le \sum_{\tau \le C(x)} \frac{x}{\tau\, C(x)^{1/2+o(1)}} = \frac{x(1 + o(1)) \log C(x)}{C(x)^{1/2+o(1)}} = \frac{x}{C(x)^{1/2+o(1)}}. \quad (3.10)$$

Finally, from (3.9) and (3.10) we get

$$A(x) \le \frac{x}{C(x)^{1/2+o(1)}},$$

as $x \to \infty$. The proof of Theorem 1.2 is complete.

Acknowledgments

The author thanks the anonymous referee for his careful reading and suggestions.

References

[1] J. J. Alba González, F. Luca, C. Pomerance, and I. E. Shparlinski, *On numbers n dividing the nth term of a linear recurrence*, Proc. Edinb. Math. Soc. **55** (2012), 271–289.

[2] R. André-Jeannin, *Divisibility of generalized Fibonacci and Lucas numbers by their subscripts*, Fibonacci Quart. **29** (1991), no. 4, 364–366.

[3] D. M. Gordon and C. Pomerance, *The distribution of Lucas and elliptic pseudoprimes*, Math. Comp. **57** (1991), no. 196, 825–838.

[4] F. Luca and E. Tron, *The distribution of self-Fibonacci divisors*, Advances in the Theory of Numbers: Proceedings of the Thirteenth Conference of the Canadian Number Theory Association (A. Alaca, Ş. Alaca, and K. S. Williams, eds.), Fields Institute Communications, Springer New York, 2015, pp. 149–158.

[5] M. Renault, *The period, rank, and order of the* (a, b)*-Fibonacci sequence* $\bmod m$, Math. Mag. **86** (2013), no. 5, 372–380.

[6] P. Ribenboim, *My numbers, my friends: Popular lectures on number theory*, Universitext - Springer-Verlag, Springer, 2000.

[7] C. Sanna, *The p-adic valuation of Lucas sequences*, Fibonacci Quart. **54** (2016), no. 2, 118–124.

[8] L. Somer, *Divisibility of terms in Lucas sequences by their subscripts*, in Applications of Fibonacci numbers, Volume 5 (1993), 515–525.

[9] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics, vol. 46, Cambridge University Press, Cambridge, 1995.