Counting divisors of Lucas numbers

Pieter Moree

Max-Planck-Institut
für Mathematik
Gottfried-Claren-Str. 26
53225 Bonn

Germany

MPI 96-34

Counting divisors of Lucas numbers

Pieter Moree

Abstract

The Lucas numbers L_n are defined by $L_0 = 2$, $L_1 = 1$ and the recurrence $L_n = L_{n-1} + L_{n-2}$. In [7] Lagarias investigated prime divisors of $\{L_n\}$. We will establish an estimate for the number of positive divisors m of $\{L_n\}$ with m not exceeding x, having an error of order $x \log^{\epsilon-1} x$ for every $\epsilon > 0$. A similar result for the sequences $\{a^n + b^n\}$ with a and b integers was established in [9].

1 Introduction

Let $\{S_n\}$ be a second order linear recurrence consisting of integers only. Several authors investigated prime divisors of such sequences, see [1] for a very readable survey. M. Ward [17] proved that, except for some degenerate cases, there are always an infinite number of distinct primes dividing the terms of $\{S_n\}$. P. J. Stephens [16] proved for a large class of second order linear recurrences that under the generalized Riemann hypothesis the set of prime divisors has a positive prime density. (If S is any set of natural numbers, then $S(x)$ denotes the number of elements n in S with $1 < n \leq x$. In case S is a set of primes we define the prime density of S to be $\lim_{x\to\infty} S(x)/\pi(x)$, if it exists, where $\pi(x)$ denotes the number of primes not exceeding x. J. C. Lagarias [7] gave sufficient conditions under which the prime density of prime divisors of a second order linear recurrence exists unconditionally and can be computed. He showed, for example, that the prime density of Lucas divisors, that is divisors of $\{L_n\}$, equals $\frac{2}{3}$. Lagarias' method goes back to H. Hasse [5] who expressed the prime density of sequences $\{a^k + b^k\}_{k=1}^{\infty}$ in terms of degrees of Kummer extensions. This method will be used in Section 3. The analytic aspects of prime divisors of sequences $\{a^k + b^k\}_{k=1}^{\infty}$ were explored by K. Wiertelak in several papers [18, 19, 20, 21, 22].

The problem of general divisors of second order linear recurrence sequences has not received much attention. Let a and b be fixed coprime integers such that $|a| \neq |b|$. In [9] the set of divisors, $G_{a,b}$, of the sequence $\{a^k + b^k\}$ was considered. The results obtained there have an application in coding theory [14]. It was shown that for given $t \geq 1$,

$$G_{a,b}(x) = \frac{x}{\log x}(c_0' \log^{\alpha} x + \sum_{j=0}^{t-1} c_{1+j}' \log^{\beta\cdot 2^{-j}} x + O(\log^{\beta\cdot 2^{-t}} x)), \qquad (1)$$

as x tends to infinity, where $c_0', \cdots, c_t'$ and α and β are positive constants depending at most on a and b. The implied constant depends at most on a, b and t. The constants

α and β can be explicitly given. They are rational numbers.

The purpose of this paper is to establish the following analogue of (1):

Theorem 1 *Let $\mathcal{L}(x)$ denote the number of divisors not exceeding x of the sequence of Lucas numbers. Then, for $t \geq 1$,*

$$\mathcal{L}(x) = \frac{x}{\log x}(\sum_{j=0}^{t-1} c_j \log^{\frac{1}{3}\cdot\frac{1}{2^j}} x + O(\log^{\frac{1}{3}\cdot\frac{1}{2^t}} x)), \tag{2}$$

where $c_0, \cdots, c_t$ are positive constants and the implied constant depends at most on t.

The sequence of exponents $\{\frac{1}{3}\cdot\frac{1}{2^j}\}_{j=0}^{\infty}$ appearing in (2) coincides with that appearing in (1) in case $a/b \neq \pm 1$, $a/b \notin \pm\mathbb{Q}^2$ and $a/b \notin \pm 2\mathbb{Q}^2$ [9].

Although the strategy of proof is similar, establishing (2) is more difficult than establishing (1). Firstly because one now has to work over the base field $\mathbb{Q}(\sqrt{5})$ rather than $\mathbb{Q}$ and secondly since many ingredients required in the proof of (1) can be found in the literature, whereas this is only rarely the case for their counterparts in the proof of (2). In order to explain the strategy of proof, a little bit of notation is needed. If $\{S_n\}$ is a sequence of integers, the smallest index k such that $m|S_k$ for some non-zero element S_k, is called the *rank of apparition* of m provided it exists. Let $\{F_n\}$ be the Fibonacci sequence. Thus $F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$, $n \geq 2$. For the Fibonacci sequence denote the rank of apparition of n by $\rho(n)$. (It exists for arbitrary n as will be seen later.) Let $\sigma(n)$ denote the rank of apparition of n in the Lucas sequence, if it exists. The proof of Theorem 1 proceeds as follows. In Section 2 a characterization for Lucas divisors is derived. This result shows the need of estimating the growth of the sets $C_e := \{p > 2 : 2^e \| \rho(p)\}$, for $e \geq 0$. Using a method of Wiertelak an estimate of the form

$$C_e(x) = \delta_e \mathrm{Li}(x) + O(\frac{x(\log\log x)^4}{\log^3 x}), \tag{3}$$

where $\delta_e > 0$ is a constant and $\mathrm{Li}(x)$ denotes the logarithmic integral, is derived. Using Hasse's method the densities δ_e are computed in Section 3. Lagarias [7] only computed δ_0; it equals $\frac{1}{3}$. Using a result on multiplicative functions that are constant on average in prime arguments, a formula for $G_e(x)$ is obtained, where G_e denotes the number of Lucas divisors not exceeding x composed only of primes from C_e. From this and the characterization of Lucas divisors it is straightforward to obtain an expression of the form (2) for *odd* Lucas divisors. Going from there to all Lucas divisors requires a bit of elementary trickery.

I would like to thank Gerhard Niklasch for an enjoyable whiteboard session and functioning as a stand-in for the LaTeX-manual. Furthermore I'd like to thank Peter Stevenhagen and many people from MPI for sharing their thoughts on how to prove Lemma 11.

2 Characterization of Lucas divisors

Put $\epsilon = \frac{1+\sqrt{5}}{2}$, $\bar{\epsilon} = \frac{1-\sqrt{5}}{2}$, $\theta = \epsilon/\bar{\epsilon}$. Note that $\theta = -\epsilon^2 = -\frac{3+\sqrt{5}}{2}$. Recall that $\mathbb{Z}[\epsilon]$ is the ring of algebraic integers of $\mathbb{Q}(\sqrt{5})$. The Fibonacci numbers F_n and the Lucas

numbers L_n satisfy

$$F_n = \frac{\epsilon^n - \bar{\epsilon}^n}{\sqrt{5}}, \; L_n = \epsilon + \bar{\epsilon}^n,$$

respectively. The symbols $p, \mathfrak{P}$ will be exclusively used to denote rational primes respectively prime ideals. In this section the prime ideals will be from $\mathbb{Z}[\epsilon]$. From elementary number theory recall that an ideal (p) is a prime ideal of degree 2 if $(5/p) = -1$, i.e. if $p \equiv \pm 2 (\mathrm{mod}\ 5)$ and $(p) = \mathfrak{P}\bar{\mathfrak{P}}$ with $\mathfrak{P}$ of degree 1 if $(5/p) = 1$, i.e. if $p \equiv \pm 1 (\mathrm{mod}\ 5)$. Furthermore $(5) = \mathfrak{P}^2$ with $\mathfrak{P} = (\sqrt{5})$. Notice that $m | F_n$ for some $n \geq 1$ if and only if $\theta^x \equiv 1 (\mathrm{mod}\ (m))$, where the congruence is in $\mathbb{Z}[\epsilon]$ and has a solution satisfying $x \geq 1$. Since θ is a unit in $\mathbb{Z}[\epsilon]$ this is the case for arbitrary m. Thus $\rho(m)$ exists. For Lucas numbers the situation is slightly more complicated. We have for $p \neq 5, \; r \geq 1$,

$$p^r | L_n \iff \theta^n \equiv -1 (\mathrm{mod}\ (p^r)) \iff \theta^n \equiv -1 (\mathrm{mod}\ \mathfrak{P}^r), \tag{4}$$

where $\mathfrak{P}$ is any prime ideal dividing (p). The $\Leftarrow$ part of the final iff statement in (4) is trivial if (p) is a prime ideal. Otherwise we have $(p) = \mathfrak{P}\bar{\mathfrak{P}}$ and $(\mathfrak{P}, \bar{\mathfrak{P}}) = 1$. By conjugation it follows from $\theta^n \equiv -1 (\mathrm{mod}\ \mathfrak{P}^r)$ that $\bar{\theta}^n \equiv -1 (\mathrm{mod}\ \bar{\mathfrak{P}}^r)$, hence $\theta^n \equiv -1 (\mathrm{mod}\ \bar{\mathfrak{P}}^r)$ and thus $\theta^n \equiv -1 (\mathrm{mod}\ (p^r))$ by the chinese remainder theorem for prime ideals. □

In the sequel we make use several times of the observation that, for $\mathfrak{P}$ of odd norm, $x^2 \equiv 1 (\mathrm{mod}\ \mathfrak{P}^r)$ has precisely the solutions $x \equiv 1 (\mathrm{mod}\ \mathfrak{P}^r)$ and $x \equiv -1 (\mathrm{mod}\ \mathfrak{P}^r)$. If it were to have another one, then both $x \pm 1 \in \mathfrak{P}$ and hence $\mathfrak{P} = (2)$, which we excluded.

Lemma 1 *Let $\mathfrak{P}$ be a prime ideal of odd norm in $\mathbb{Z}[\epsilon]$ and $r \geq 1$. Let $\psi \in \mathbb{Q}(\sqrt{5})$ with $(\psi, \mathfrak{P}) = 1$. Then $\psi^e \equiv -1 (\mathrm{mod}\ \mathfrak{P}^r)$ for some e if and only if $ord_{\mathfrak{P}^r}(\psi)$ is even. In case $ord_{\mathfrak{P}^r}(\psi)$ is even, the smallest e such that $\psi^e \equiv -1 (\mathrm{mod}\ \mathfrak{P}^r)$ equals $ord_{\mathfrak{P}^r}(\psi)/2$. Furthermore,*

$$\theta^f \equiv -1 (\mathrm{mod}\ \mathfrak{P}^r) \iff f \equiv \mathrm{ord}_{\mathfrak{P}^r}(\psi)/2 \ (\mathrm{mod}\ \mathrm{ord}_{\mathfrak{P}^r}(\psi)). \tag{5}$$

Proof: Suppose that -1 can be represented as a power of ψ modulo $\mathfrak{P}^r$. Let e be the smallest number such that $\psi^e \equiv -1 (\mathrm{mod}\ \mathfrak{P}^r)$. Clearly $\mathrm{ord}_{\mathfrak{P}^r}(\psi)$ cannot be a divisor of e. Thus $\mathrm{ord}_{\mathfrak{P}^r}(\psi) = 2c$ for some c dividing e. Since $\psi^c \not\equiv 1 (\mathrm{mod}\ \mathfrak{P}^r)$, we must have $\psi^c \equiv -1 (\mathrm{mod}\ \mathfrak{P}^r)$ and thus by the minimality of e, $c = e$. Thus $\mathrm{ord}_{\mathfrak{P}^r}(\psi)$ is even and $e = \mathrm{ord}_{\mathfrak{P}^r}(\psi)/2$.

On the other hand if $\mathrm{ord}_{\mathfrak{P}^r}(\psi)$ is even, then ψ^e with $e = \mathrm{ord}_{\mathfrak{P}^r}(\psi)/2$ is a solution $\not\equiv 1 (\mathrm{mod}\ \mathfrak{P}^r)$ of $x^2 \equiv 1 (\mathrm{mod}\ \mathfrak{P}^r)$ and thus $\psi^e \equiv -1 (\mathrm{mod}\ \mathfrak{P}^r)$. Suppose that $\psi^f \equiv -1 (\mathrm{mod}\ \mathfrak{P}^r)$ and f is not a multiple of e. Then $2(f, e) < 2e = \mathrm{ord}_{\mathfrak{P}^r}(\psi)$ and $\theta^{2(e,f)} \equiv 1 (\mathrm{mod}\ \mathfrak{P}^r)$. This contradiction shows that f must be a multiple of e. It is obvious that f must be an odd multiple of e and that this is also sufficient. □

Lemma 2 *Let p be a prime, $\mathfrak{P}|(p)$. Then $\rho(p^r) = \mathrm{ord}_{\mathfrak{P}^r}(\theta)$, except when $p = 5$ in which case $\rho(5^r) = 5^r$ for $r \geq 1$.*

Proof: Analogously to (4), $p^r|F_n$ iff $\theta^n \equiv 1(\text{mod } \mathfrak{P}^r)$, in case $p \neq 5$. Thus $\rho(p^r) = \text{ord}_{\mathfrak{P}^r}(\theta)$. The latter part of the assertion is left as an exercise to the reader. □

By (4), Lemma 1 and Lemma 2 we have:

Lemma 3 *The odd prime power p^r is a divisor of $\{L_n\}$ if and only if $\rho(p^r)$ is even. If p^r is a divisor of $\{L_n\}$ then $\sigma(p^r) = \rho(p^r)/2$ and*

$$p^r|L_n \iff n \equiv \rho(p^r)/2 \text{ (mod } \rho(p^r)). \tag{6}$$

Lemma 4 *If $\mathfrak{P}$ is of degree 1, then $ord_{\mathfrak{P}}(\theta)|p-1$, if $\mathfrak{P}$ is of degree 2, then $ord_{\mathfrak{P}}(\theta)|p+1$.*

Proof: Since $\mathbb{Z}[\epsilon]/\mathfrak{P} \cong \mathbb{F}_p$ when $\mathfrak{P}$ is of degree 1 and $\mathbb{F}_p^*$ is cyclic of order $p-1$, the first part of the assertion follows. In the second case we have $\mathbb{Z}[\epsilon]/\mathfrak{P} \cong \mathbb{F}_{p^2}$. Recall that $\mathbb{F}_p^* \cong \{\psi^{p+1} : \psi \in \mathbb{F}_{p^2}^*\}$ and that $\theta = -\epsilon^2$. Thus $\theta^{\frac{p+1}{2}} = (-)^{\frac{p+1}{2}}\epsilon^{p+1} \equiv c(\text{mod } p)$ for some integer c. Conjugating we find that $\bar{\theta}^{\frac{p+1}{2}} \equiv c(\text{mod } p)$. Thus $1 = (\theta\bar{\theta})^{\frac{p+1}{2}} \equiv c^2(\text{mod } p)$ and so $\theta^{p+1} \equiv 1(\text{mod } \mathfrak{P})$. □

Noting that $\rho(5) = 5$ and that for $p \neq 5$, $N(\mathfrak{P}) = p^{\frac{3-(5/p)}{2}}$, with $(5/p)$ the Legendre symbol, we find from Lemma 4 the classical result due to Lucas that $\rho(p)$ divides $p - (5/p)$.

The next proposition relates $\rho(p^r)$ to $\rho(p)$.

Proposition 1 *Let p^r be an odd prime power. Then for some $0 \leq j \leq r-1$, $\rho(p^r) = \rho(p)p^j$.*

Proof: By Lemma 2 the result holds for $p = 5$. Assume $p \neq 5$. Then, by Lemma 2 $\rho(p^r) = \text{ord}_{\mathfrak{P}^r}(\theta)$, where $\mathfrak{P}$ is a prime ideal dividing (p). We have $\theta^{\rho(p)} \equiv 1(\text{mod } \mathfrak{P})$ and, using induction and the binomial theorem, $\theta^{\rho(p)p^{r-1}} \equiv 1(\text{mod } \mathfrak{P}^r)$. Thus $\rho(p^r)|\rho(p)p^{r-1}$ so $\rho(p^r) = cp^j$ for some $c|\rho(p)$ and $0 \leq j \leq r-1$. In case $\mathfrak{P}$ is of degree 1, we have $\theta^p \equiv \theta(\text{mod } \mathfrak{P})$ by Lemma 4. Then, since $1 \equiv \theta^{cp^j} \equiv \theta^c(\text{mod } \mathfrak{P})$, $c = \text{ord}_{\mathfrak{P}}(\theta) = \rho(p)$. In case $\mathfrak{P}$ is of degree 2, we have $\theta^p \equiv \frac{1}{\theta}(\text{mod } \mathfrak{P})$ by Lemma 4. Again it follows that $1 \equiv \theta^c(\text{mod } \mathfrak{P})$ and hence $c = \text{ord}_{\mathfrak{P}}(\theta) = \rho(p)$. □

In order to prove the main result of this section we need one more lemma.

Lemma 5 [9] *Let $a_1, \ldots, a_k$ be natural numbers. The system of congruences*

$$x \equiv a_1(\text{mod } 2a_1), \cdots, x \equiv a_i(\text{mod } 2a_i), \cdots, x \equiv a_k(\text{mod } 2a_k)$$

has a solution x iff there exists $e \geq 0$ such that $2^e||a_i$ for $1 \leq i \leq k$.

Theorem 2 *An odd integer m divides $\{L_n\}$ if and only if there exists $e \geq 1$ such that $2^e||\rho(p)$, the rank of apparition of p in $\{F_n\}$, for every prime p dividing m.*

Proof: Note that by Lemma 2 we may assume that $(m, 5) = 1$. '$\Rightarrow$'. Let m be an odd divisor of $\{L_n\}$. Let $p_1, \cdots, p_k$ be its prime divisors. Define e_i by $p_i^{e_i}||m$. Choose prime ideals $\mathfrak{P}_1, \cdots, \mathfrak{P}_k$ lying over p_i for $1 \leq i \leq k$. By (6) there exists c such that $\theta^c \equiv -1(\text{mod } \mathfrak{P}_i^{e_i})$ for $1 \leq i \leq k$. Now using Lemma 1, we obtain that $\text{ord}_{\mathfrak{P}_i{}^{e_i}}(\theta)$ is even and

$$c \equiv \text{ord}_{\mathfrak{P}_i{}^{e_i}}(\theta)/2 \text{ (mod ord}_{\mathfrak{P}_i{}^{e_i}}(\theta)), \ 1 \leq i \leq k. \tag{7}$$

Lemma 5 with $a_i = \mathrm{ord}_{\mathfrak{P}_i^{e_i}}(\theta)/2$, $1 \le i \le k$ and Lemma 2 then yields the existence of an $e \ge 1$ such that $2^e \| \rho(p_i^{e_i})$ for $1 \le i \le k$. The implication '$\Rightarrow$' then follows on using Proposition 1.

'$\Leftarrow$'. By assumption, Proposition 1 and Lemma 2, there exists $e \ge 1$ such that $2^e \| \mathrm{ord}_{\mathfrak{P}_i^{e_i}}(\theta)$ for $1 \le i \le k$. By Lemma 5 there exists an integer c satisfying $c \equiv \mathrm{ord}_{\mathfrak{P}_i^{e_i}}(\theta)/2 \pmod{\mathrm{ord}_{\mathfrak{P}_i^{e_i}}(\theta)}$ for $1 \le i \le k$. Thus, by (5), $\theta^c \equiv -1 \pmod{\mathfrak{P}_i^{e_i}}$ for $1 \le i \le k$ and hence, by (4), $\theta^c \equiv -1 \pmod{(m)}$ and $m | L_c$. □

3 Computing the densities δ_e

In order to prove the estimate (3) we need to compute, for $e \ge 0$, the prime density δ_e of the set $C_e := \{p > 2 : 2^e \| \rho(p)\}$. This can be almost carried out by algebraic number theory only. For $s = 1, 2$, $e \ge 0$, $j \ge 1$ put

$$N_s(e,j) = \{p : p \equiv \pm s \pmod 5,\ p \equiv 3 - 2s + 2^j \pmod{2^{j+1}},\ 2^e \| \mathrm{ord}_{(p)}(\theta)\}.$$

Then it follows on using Lemma 2 that $C_0 = \cup_{j=1}^{\infty}\{N_1(e,j) \cup N_2(e,j)\} \cup \{5\}$ and $C_e = \cup_{j=1}^{\infty}\{N_1(e,j) \cup N_2(e,j)\}$ for $e \ge 1$. Note that all sets in this union are disjoint. As a first step we compute $\Delta_s(e,j)$, the prime density of the set $N_s(e,j)$. In the case $s = 1$ this problem can be reduced to computing degrees of certain number fields. This reduction is due to Hasse [5] and was used by several subsequent authors [1, 7, 12, 18]. The case $s = 2$ is almost trivial; here one only needs the prime number theorem for arithmetic progressions. The densities $\Delta_1(e,j)$, $\Delta_2(e,j)$ are recorded in Table 1 and Table 2 respectively. The entry e in the last column gives $\sum_{j=1}^{\infty} \Delta_s(e,j)$. The entry j in the last row gives $\sum_{e=0}^{\infty} \Delta_s(e,j)$.

The case $s = 1$. Here some some information on the number fields $K_{0,n} := \mathbb{Q}(\sqrt{5}, \zeta_{2^n})$, $n \ge 1$, is needed. $K_{0,n}$ is normal over $\mathbb{Q}$ as it is isomorphic to the splitting field of $(X^{2^n} - 1)(X^2 - 5)$. It is of degree 2^n over $\mathbb{Q}$. As is well-known the absolute value of the discriminant of $\mathbb{Q}(\zeta_{2^n})$ is $(m/2)^{m/2}$, where $m = 2^n$. The discriminant of $\mathbb{Q}(\sqrt{5})$ is 5. Now if $K \subseteq L \subseteq M$ is a tower of fields, then (see e.g. [11, Proposition 4.9])

$$d_{M/K} = (N_{L/K} d_{M/L}) d_{L/K}^{[M:L]}. \tag{8}$$

Thus the absolute value of the discriminant of $K_{0,n}$ equals $5^{m/2}(m/2)^m$ and consequently the primes outside $\{2, 5\}$ do not ramify. The primes that split completely in $K_{0,n}$ are precisely the primes satisfying $p \equiv \pm 1 \pmod 5$ and $p \equiv 1 \pmod{2^n}$.

Lemma 6 *Put* $K_{a,b} = \mathbb{Q}(\sqrt{5}, \theta^{1/2^a}, \zeta_{2^b})$. *Then, for* $b > a \ge 1$,

$$d_{a,b} := [K_{a,b} : \mathbb{Q}] = 2^{a+b-1}.$$

Furthermore $d_{0,b} = 2^b$, $b \ge 1$, $d_{1,1} = 4$ *and* $d_{b,b} = 2^{2b-1}$ *for* $b \ge 2$.

Proof: When $b > a \ge 1$, $K_{a,b} = \mathbb{Q}(\sqrt{5}, \epsilon^{1/2^{a-1}} \zeta_{2^{a+1}}, \zeta_{2^b}) = \mathbb{Q}(\epsilon^{1/2^{a-1}}, \zeta_{2^b})$. Using the well-known fact that $\mathbb{Q}(\zeta_{2^b})$ contains at most the quadratic subfields $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$, the fields $\mathbb{Q}(\epsilon^{1/2^{a-1}})$ and $\mathbb{Q}(\zeta_{2^b})$ are seen to be linearly disjoint and hence

$$d_{a,b} = [\mathbb{Q}(\epsilon^{1/2^{a-1}}) : \mathbb{Q}][\mathbb{Q}(\zeta_{2^b}) : \mathbb{Q}] = 2^{a+b-1}.$$

The claim on $d_{0,b}$ is almost immediate, that on $d_{b,b}$ is proved in [7, Lemma 3.1]. □

Lemma 7 *A prime p satisfies*

$$p \equiv \pm 1 (\mathrm{mod}\ 5),\ p \equiv 1 + 2^j (\mathrm{mod}\ 2^{j+1}),\ \theta^{\frac{p-1}{2^t}} \equiv 1 (\mathrm{mod}\ \mathfrak{P}), \tag{9}$$

where $t \leq j$ and $\mathfrak{P}$ is a prime ideal in $\mathbb{Z}[\epsilon]$ dividing (p) if and only if p splits completely in $K_{t,j}$, but does not split completely in $K_{t,j+1}$. The prime density of the set of all primes satisfying (9) equals $\frac{1}{d_{t,j}} - \frac{1}{d_{t,j+1}}$.

Proof: Suppose that p satisfies (9). Then p splits completely in $K_{0,j}$. Furthermore $\theta^{\frac{p-1}{2^t}} \equiv 1 (\mathrm{mod}\ \mathfrak{P})$ implies by Euler's criterion that $x^{2^t} \equiv \theta (\mathrm{mod}\ \mathfrak{P})$ has a solution mod $\mathfrak{P}$. Let $\mathfrak{Q}$ be a prime ideal of $\mathfrak{O}_{K_{e,j}}$ lying over $\mathfrak{P}$. Since the inertial degree $f(\mathfrak{Q}|\mathfrak{P}) = 1$, $x^{2^t} \equiv \theta (\mathrm{mod}\ \mathfrak{P})$ has a solution mod $\mathfrak{P}$ iff $x^{2^t} \equiv \theta (\mathrm{mod}\ \mathfrak{Q})$ has a solution mod $\mathfrak{Q}$. Using the Kummer-Dedekind theorem in the formulation of Pohst and Zassenhaus [15, p. 390], together with part (b) of the Lemma at p. 392 and the fact that the discriminant of $K_{t,j}$ contains no prime factors outside the set $\{2, 5\}$, it follows that $\mathfrak{Q}$ splits in $K_{t,j}$. For $t = 0$, $K_{t,j}$ is normal over $\mathbb{Q}$ as has been remarked before, for $t \geq 1$ it is the splitting field of $(X^{2^j} - \theta^{2^{j-t}})(X^{2^j} - \bar{\theta}^{2^{j-t}}) \in \mathbb{Z}[X]$ and hence also normal over $\mathbb{Q}$. That means that p splits completely in $K_{t,j}$. Since $p \not\equiv 1 (\mathrm{mod}\ 2^{j+1})$, p does not split completely in $K_{t,j+1}$. The proof of the reverse equivalence should be evident to the reader now. The proof of the last part of the assertion follows from the Chebotarev density theorem. □

The next lemma gives the densities $\Delta_1(e, j)$ for $e \geq 0$ and $j \geq 1$. For the convenience of the reader these prime densities are recorded in Table 1.

Lemma 8 $\Delta_1(e, j) = 0$ *for* $e > j$. $\Delta_1(0, 1) = 0$, $\Delta_1(0, j) = 1/4^j$ *for* $j \geq 2$. *For* $j \geq 1$, $\Delta_1(1, j) = 1/4^j$. *For* $j \geq 2$, $\Delta_1(j, j) = 0$. $\Delta_1(e, j) = 1/2^{2j+1-e}$ *for* $e \geq 2$ *and* $j \geq e + 1$.

Proof: Suppose that $p \in N_1(e, j)$. By (4) the assertion $2^e \| \mathrm{ord}_{(p)}(\theta)$ is equivalent with

$$2^e \| \mathrm{ord}_{\mathfrak{P}}(\theta), \tag{10}$$

where $\mathfrak{P}|(p)$. The first part of the assertion is immediate by Lemma 4. So assume $e \leq j$. In case $e = 0$ the condition (10) is equivalent with $\theta^{\frac{p-1}{2^j}} \equiv 1 (\mathrm{mod}\ \mathfrak{P})$. Then, by Lemma 7, $\Delta_1(0, j) = 1/d_{j,j} - 1/d_{j,j+1}$. Using Lemma 6 we find $\Delta_1(0, 1) = 0$ and $\Delta_1(0, j) = 1/4^j$ for $j \geq 2$. In case $e \geq 1$ the condition (10) is equivalent with $\theta^{\frac{p-1}{2^{j-e}}} \equiv 1 (\mathrm{mod}\ \mathfrak{P})$ and $\theta^{\frac{p-1}{2^{j-e+1}}} \not\equiv 1 (\mathrm{mod}\ \mathfrak{P})$. Thus, using Lemma 7, we find that for $e \geq 1$, $e \leq j$,

$$\Delta_1(e, j) = \frac{1}{d_{j-e,j}} - \frac{1}{d_{j-e,j+1}} - \frac{1}{d_{j+1-e,j}} + \frac{1}{d_{j+1-e,j+1}}.$$

The remainder of the assertion now follows on invoking Lemma 6. □

The case $s = 2$. Let $p \equiv \pm 2 (\mathrm{mod}\ 5)$. Recall that $\mathrm{ord}_{(p)}(\theta) | p+1$. Since $\epsilon^p \equiv \bar{\epsilon} (\mathrm{mod}\ (p))$ and $\epsilon\bar{\epsilon} = -1$, $\epsilon^{p+1} \equiv -1 (\mathrm{mod}\ (p))$. Hence if $p \equiv -1 + 2^j (\mathrm{mod}\ 2^{j+1})$, $j \geq 2$, then $\theta^{\frac{p+1}{2}} = (-1)^{\frac{p+1}{2}} \epsilon^{p+1} \equiv -1 (\mathrm{mod}\ (p))$. Thus $2^j \| \mathrm{ord}_{(p)}(\theta)$ and therefore $N_2(j,j) = \{p : p \equiv \pm 2 (\mathrm{mod}\ 5),\ p \equiv -1 + 2^j (\mathrm{mod}\ 2^{j+1})\}$. In particular $\Delta_2(j,j) = \frac{1}{2^{j+1}}$ and $\Delta_2(e,j) = 0$ when $e \neq j$. In case $j = 1$ and $p \equiv 1 (\mathrm{mod}\ 4)$, then $\theta^{\frac{p+1}{2}} = (-1)^{\frac{p+1}{2}} \epsilon^{p+1} \equiv 1 (\mathrm{mod}\ (p))$. Thus, since $(p+1)/2$ is odd, $N_2(0,1) = \{p : p \equiv \pm 2 (\mathrm{mod}\ 5), p \equiv 1 (\mathrm{mod}\ 4)\}$, $\Delta_2(0,1) = 1/4$ and, for $e \geq 1$, $\Delta_2(e,1) = 0$. This finishes the computation of the densities $\Delta_2(e,j)$. They are recorded in Table 2.

The analytic arguments in the next section will show that $\delta_e = \sum_{j=1}^{\infty} \{\Delta_1(e,j) + \Delta_2(e,j)\}$. Using the formulae derived in this section for the prime densities $\Delta_1(e,j)$ and $\Delta_2(e,j)$ it then follows that

$$\delta_0 = \frac{1}{3},\ \delta_e = \frac{2}{3} \cdot \frac{1}{2^e}\ (e \geq 1).$$

4 Counting primes dividing Lucas numbers

In this section Theorem 3 will be proved following Wiertelak [18], who on his turn used some ideas of P. D. T. A. Elliott [3]. Wiertelak used character sums over prime ideals to evaluate $W_m(x)$, where $W_m := \{p : m | \mathrm{ord}_p(a/b)\}$, with a and b non-zero integers. A slightly easier alternative approach to deal with $W_m(x)$, as explored by R. W. K. Odoni [12], would only yield an error of $\exp\{-c \log\log x / \log\log\log x\}$, for some constant $c > 0$, which, however, is not sharp enough for our purposes.

Theorem 3 *Let $\rho(p)$ denote the rank of apparition of p in the Fibonacci sequence. For $e \geq 0$ put $C_e = \{p > 2 : 2^e \| \rho(p)\}$. Then*

$$C_e(x) = \delta_e \mathrm{Li}(x) + O(\frac{x(\log\log x)^4}{\log^3 x}),$$

where $\delta_0 = \frac{1}{3}$, $\delta_e = \frac{2}{3} \cdot \frac{1}{2^e}$ for $e \geq 1$ and the implied constant may depend on e.

This result together with Theorem 2 and the prime number theorem with error $O(x \log^{-3} x)$ implies the following improvement of [7, Theorem B]:

Theorem 4 *The set of prime divisors of the sequence of Lucas numbers, $\mathcal{P}$, satisfies*

$$\mathcal{P}(x) = \frac{2}{3}\mathrm{Li}(x) + O(\frac{x(\log\log x)^4}{\log^3 x}).$$

In particular the set $\mathcal{P}$ has prime density $\frac{2}{3}$.

Before embarking on the proof of Theorem 3 we need a few prerequisites.

Let K be a number field of discriminant $d_{K/\mathbb{Q}}$ and degree n over the rationals. Let $\mathcal{O}_K$ be its ring of integers, $\mathfrak{A}$ an arbitrary integral ideal and $\mathfrak{P}$ an arbitrary integral prime ideal. Let χ be a character of the group of ideal classes modulo $\mathfrak{A}$ and $\zeta(s,\chi)$ the Hecke zeta function (see [8]). By the group of ideal classes modulo $\mathfrak{A}$ we understand

the following. We say that $\mathfrak{B} \sim \mathfrak{B}' (\mathrm{mod}\ \mathfrak{A})$ iff $(\mathfrak{B}, \mathfrak{A}) = (\mathfrak{B}', \mathfrak{A}) = 1$ and there exist totally positive ξ and δ in $\mathfrak{O}_K$ such that $\xi \equiv \delta \equiv 1 (\mathrm{mod}\ \mathfrak{A})$ and $(\xi)\mathfrak{B} = (\delta)\mathfrak{B}'$. The principal character of the group of ideal classes modulo $\mathfrak{A}$ will be denoted by χ_0, the exceptional real character by χ_1 and the hypothetical Siegel zero of $\zeta(s, \chi_1)$, which is real and simple, by β_1. We denote the product of $|d_{K/\mathbb{Q}}|$ and $N\mathfrak{A}$, the norm of $\mathfrak{A}$, by Δ. Set $E_0(\chi) = 1$ if $\chi = \chi_0$ is the principal character and zero otherwise. Set $E_1(\chi) = 1$ if $\chi = \chi_1$ is the exceptional real character and zero otherwise.

Lemma 9 [18] *There exists an absolute positive constant g_1 such that*

$$\sum_{N\mathfrak{P} \le x} \chi(\mathfrak{P}) = E_0(\chi)\mathrm{Li}(x) - E_1(\chi)\mathrm{Li}(x^{\beta_1}) + O(R),$$

where

$$R = \frac{x \log(2\Delta)}{\sqrt{\log x}} \exp\{-g_1 \frac{\log x}{\max\{\sqrt{n \log x}, \Delta\}}\}$$

and the implied constant and g_1 are absolute.

A similar estimate for more general characters can be found in a paper of B. Z. Moroz [10].

Lemma 10 [18] *Let K be normal over $\mathbb{Q}$. Then for any $\epsilon > 0$ there exists $C(\epsilon)$ such that*

$$\beta_1 < \max\Big(1 - \frac{1}{32 \log(\Delta \sqrt{N\mathfrak{A}})}, 1 - \frac{C(\epsilon)}{(\Delta \sqrt{N\mathfrak{A}})^{\epsilon/n}}\Big).$$

Let $m > 1$ be an integer. Put $L = K(\zeta_m)$. For $\psi \in \mathfrak{O}_K$ and a prime ideal $\mathfrak{P}$ of $\mathfrak{O}_L$, $(\mathfrak{P}, m\psi) = 1$, we denote by $\left(\frac{\psi}{\mathfrak{P}}\right)_m$ the mth power residue symbol. It is the unique mth root of unity such that $\left(\frac{\psi}{\mathfrak{P}}\right)_m \equiv \alpha^{\frac{N\mathfrak{P}-1}{m}} (\mathrm{mod}\ \mathfrak{P})$. For the ideal $\mathfrak{A}$ of $\mathfrak{O}_L$, $(\mathfrak{A}, m\psi) = 1$, we put

$$\left(\frac{\psi}{\mathfrak{A}}\right)_m = \prod_{p^w \| \mathfrak{A}} \left(\frac{\psi}{\mathfrak{P}}\right)_m^w.$$

Lemma 11 *Let $m > 1$ be an integer. Let K be a number field. Let $\alpha \in \mathfrak{O}_K$, $\alpha \neq 0$. If $\mathfrak{B}$ and $\mathfrak{B}'$ are ideals of $\mathfrak{O}_{K(\zeta_m)}$ coprime to $(m^3\alpha)$ and $\mathfrak{B}'\mathfrak{B}^{-1} = (c)$, where c is totally positive and $c \equiv 1((m^3\alpha))$, then*

$$\left(\frac{\alpha}{\mathfrak{B}'}\right)_m = \left(\frac{\alpha}{\mathfrak{B}}\right)_m.$$

Proof. The proof easily follows on combining [2, Exercise 1.8] and [6, Satz 121]. An alternative proof arises on using the well-known fact that $\left(\frac{\alpha}{\mathfrak{P}}\right)_m$ depends only on the class to which $\mathfrak{P}$ belongs mod $\mathfrak{f}$, where $\mathfrak{f}$ is the conductor of $K(\zeta_m, \alpha^{1/m})$ (see e.g. [2, p. 273]). The proof then follows on using an estimate due to Hasse for the conductor of Kummerian fields ([6, Satz 166]; the meaning of the symbols ν and s_0 appearing in Satz 166 is explained in Satz 164). □

Lemma 11 was proved in case $K = \mathbb{Q}$ by Elliott [4] with $m^3\alpha$ replaced by $m^2\alpha$.

Elliott made heavy use of classical reciprocity results due to Hasse. The point of Lemma 11 is that it shows that the conductor of $K(\alpha^{1/m})$, viewed as a function of m, is polynomial in m. A trivial estimate for the conductor is provided by the discriminant (since the conductor divides the discriminant) and hence is $O(m^m)$. Usage of this estimate would result in a larger error term in Theorem 3.

Implicit error terms appearing in the remainder of this section that are not subindexed may depend at most on ψ and K.

Theorem 5 *Let K be a normal extension of $\mathbb{Q}$, $\psi \in \mathfrak{O}_K$ and $M = K(\zeta_{2^n}, \psi^{1/2^r})$. Let $\pi_M(x)$ denote the number of rational primes not exceeding x that split completely in M. Then for any $C > 0$ there exists a constant $g_2 > 0$ depending at most on ψ, K and C, such that*

$$\pi_M(x) = \frac{\mathrm{Li}(x)}{[M:\mathbb{Q}]} + O(\frac{x}{\log^C x}),$$

uniformly for

$$2^n \leq g_2 \frac{\log x}{(\log\log x)^2}, \ r \leq n. \tag{11}$$

The implied constant also depends at most on ψ, K and C.

Proof of Theorem 5. Put $L = K(\zeta_n)$ and $M = L(\psi^{\frac{1}{2^r}})$. For the duration of this proof $\mathfrak{P}$ will be used to denote a prime ideal from $\mathfrak{O}_L$. Note that L as a compositum of two normal extension of $\mathbb{Q}$ is itself normal over $\mathbb{Q}$. Let $r \leq n$. Let S_M denote the set of primes

$$\{p : (p, 2N_{K/\mathbb{Q}}(\psi)) = 1, \ p \ \text{splits completely in } L, \ X^{2^r} \equiv \psi (\mathrm{mod}\ \mathfrak{P}), \mathfrak{P}|(p)\}.$$

Using the Kummer-Dedekind theorem [15, p. 390], together with part (b) of the Lemma on p. 392 and the fact that the prime divisors of $d_{M:\mathbb{Q}}$ depend at most on ψ and K, it follows that

$$\pi_M(x) = S_M(x) + O(1). \tag{12}$$

Since for p in S_M, $N\mathfrak{P} = p \equiv 1 (\mathrm{mod}\ 2^r)$, we can by the Euler criterion also write

$$\{p : (p, 2N_{K/\mathbb{Q}}(\psi)) = 1, \ p \ \text{splits completely in } L, \ \psi^{\frac{p-1}{2^r}} \equiv 1 (\mathrm{mod}\ \mathfrak{P}), \mathfrak{P}|(p)\}$$

for S_M. On using the power residue symbol we can finally write

$$S_M = \{p : (p, 2N_{K/\mathbb{Q}}(\psi)) = 1, \ p \ \text{splits completely in } L, (\frac{\psi}{\mathfrak{P}})_{2^r} = 1, \mathfrak{P}|(p)\}.$$

Now let us define $T_{M,1} = \{\mathfrak{P} : (\mathfrak{P}, 2^n\psi) = 1, \ \left(\frac{\psi}{\mathfrak{P}}\right)_{2^r} = 1, \ f(\mathfrak{P}|p) = 1\}$ and $T_M = \{\mathfrak{P} : (\mathfrak{P}, 2^n\psi) = 1, \ \left(\frac{\psi}{\mathfrak{P}}\right)_{2^r} = 1\}$. Using that L is normal over $\mathbb{Q}$ it follows that $S_M(x) = T_{M,1}(x)/[L:\mathbb{Q}] + O(1)$. Since $T_M(x) = T_{M,1}(x) + O([L:\mathbb{Q}]\sqrt{x}\log x)$, we find

$$S_M(x) = \frac{T_M(x)}{[L:\mathbb{Q}]} + O(\sqrt{x}\log x). \tag{13}$$

Next we estimate $T_M(x)$. Let ϵ_k be a primitive kth root of unity. Note that

$$\frac{1}{k}\sum_{j=1}^{k}(\left(\frac{\alpha}{\mathfrak{P}}\right)_k/\epsilon_k)^j = \begin{cases} 1 & \text{if } \left(\frac{\alpha}{\mathfrak{P}}\right)_k = \epsilon_k; \\ 0 & \text{otherwise.} \end{cases}$$

Using this with $k = 2^r$ and $\alpha = \psi$ we obtain

$$T_M(x) = \sum_{N\mathfrak{P}\le x,\ \left(\frac{\psi}{\mathfrak{P}}\right)_{2^r}=1} 1 = \frac{1}{2^r}\sum_{j=1}^{2^r}\frac{1}{\epsilon_{2^r}^j}\sum_{N\mathfrak{P}\le x}\left(\frac{\psi^j}{\mathfrak{P}}\right)_{2^r}, \tag{14}$$

where the summation is over all prime ideals $\mathfrak{P}$ in $\mathfrak{O}_L$ satisfying $(\mathfrak{P}, 2^n\psi) = 1$. For a given integer $1 \le j \le 2^r$ we define $\chi_j(\mathfrak{A})$ to be $\left(\frac{\psi^j}{\mathfrak{A}}\right)_{2^n}^{2^{n-r}}$ in case $(\mathfrak{A}, 8^n\psi) = 1$ and zero otherwise. Thus we can rewrite (14) as

$$T_M(x) = \frac{1}{2^r}\sum_{j=1}^{2^r}\frac{1}{\epsilon_{2^r}^j}\sum_{N\mathfrak{P}\le x}\chi_j(\mathfrak{P}).$$

From this, Lemma 10, (13) and (12) we obtain

$$\pi_M(x) = \frac{a_M}{[L:\mathbb{Q}]}\mathrm{Li}(x) - \frac{b_M}{[L:\mathbb{Q}]}\mathrm{Li}(x^{\beta_1}) + O(R) + O(\sqrt{x}\log x), \tag{15}$$

with $0 \le |a_M|, |b_M| \le 1$, R as in Lemma 10 and $\Delta = |d_{M/\mathbb{Q}}| \cdot N_{L\setminus\mathbb{Q}}(8^n\psi)$. If r and n satisfy (11) then

$$\log\Delta \le g_1 g_3 2^n n, \tag{16}$$

where g_3 depends at most on ψ and K. Let $C > 0$ be given. Using the estimate (16) and Lemma 10 to deal with the exceptional zero β_1 in (15), we see that we can choose g_1 so small as to ensure that $\pi_M(x) = \frac{a_M}{[L:\mathbb{Q}]}\mathrm{Li}(x) + O(x\log^{-C}x)$ uniformly in the region (11). By the Chebotarev density theorem it follows that $a_M/[L:\mathbb{Q}] = 1/[M:\mathbb{Q}]$ (hence $a_M = 1/[M:L]$). So the result follows. □

It should be remarked that the best known uniform version of the Chebotarev theorem yields only a far weaker result (cf. [12]). Our approach, however, does not work for arbitrary number fields and hence does not lead to a better uniform version of the Chebotarev density theorem.

Proof of Theorem 3. Applying Theorem 5 to $K = \mathbb{Q}(\sqrt{5})$ and $\psi = -\frac{3+\sqrt{5}}{2}$, we find using Lemma 7 that there exists an absolute positive constant g_4 such that uniformly for $2^j \le g_4\log x(\log\log x)^{-2}$, $e \le j$,

$$N_1(e,j)(x) = \Delta_1(e,j)\mathrm{Li}(x) + O(\frac{x}{\log^3 x}). \tag{17}$$

Next we estimate $I(x) := \sum_{j=1}^{\infty} N_1(e,j)(x)$. Since $N_1(e,j)$ is empty for $j < e$, we can write $I(x) = I_1(x) + I_2(x)$, where $I_1(x) = \sum_{j=e}^{m} N_1(e,j)(x)$, $I_2(x) = \sum_{j=m+1}^{\infty} N_1(e,j)(x)$

and m is the largest integer such that $2^m \leq g_4 \log x (\log\log x)^{-2}$. Using equation (17) and $\Delta_1(e,j) \ll 1/4^j$ (see Lemma 8) we find

$$\begin{aligned} I_1(x) &= \{\sum_{j=r}^{m} \Delta_1(e,j)\}\mathrm{Li}(x) + O(m\frac{x}{\log^3 x}) \\ &= \{\sum_{j=1}^{\infty} \Delta_1(e,j)\}\mathrm{Li}(x) + O(\frac{\mathrm{Li}(x)}{4^m}) + O(m\frac{x}{\log^3 x}) \\ &= \{\sum_{j=1}^{\infty} \Delta_1(e,j)\}\mathrm{Li}(x) + O(\frac{x(\log\log x)^4}{\log^3 x}). \end{aligned}$$

The primes counted by $I_2(x)$ all satisfy the congruences $p \equiv \pm 1 (\mathrm{mod}\ 5)$, $p \equiv 1(\mathrm{mod}\ 2^m)$ and $\theta^{(p-1)/2^m} \equiv 1 (\mathrm{mod}\ \mathfrak{P})$, where $\mathfrak{P}|(p)$. Thus $I_2(x) \leq \pi_{K_{m,m}}(x)$ (cf. the proof of Lemma 7). By Lemma 6 $[K_{m,m} : \mathbb{Q}] \gg 4^m$. It follows from this estimate, Theorem 5 and $2^m \leq g_4(\log x)(\log\log x)^{-2}$ that $I_2(x) = O(x(\log\log x)^4 \log^{-3} x)$. Thus

$$I(x) = \{\sum_{j=1}^{\infty} \Delta_1(e,j)\}\mathrm{Li}(x) + O(\frac{x(\log\log x)^4}{\log^3 x}).$$

Put $J(x) = \sum_{j=1}^{\infty} N_2(e,j)(x)$. In every row in Table 2 there is at most one non-zero prime density. As was seen in the computation of the prime densities $\Delta_2(e,j)$, the set corresponding to the non-zero prime density consists of all primes in a finite union of arithmetic progressions and furthermore the sets corresponding to the zero prime densities are all empty. Hence it follows using the prime number theorem for arithmetic progressions that

$$J(x) = \{\sum_{j=1}^{\infty} \Delta_2(e,j)\}\mathrm{Li}(x) + O(\frac{x}{\log^3 x}).$$

Thus

$$P_e(x) = \{\sum_{j=1}^{\infty} \Delta_1(e,j) + \Delta_2(e,j))\}\mathrm{Li}(x) + O(\frac{x(\log\log x)^4}{\log^3 x})$$

and on recalling the conclusion of Section 3, the proof of Theorem 3 becomes complete.

5 Counting Lucas divisors

Once Theorem 3 is established it is rather straightforward to prove Theorem 1, which will be done in this section. Recall that $\delta_j = \frac{2}{3} \cdot \frac{1}{2^j}$, $j \geq 1$. Let $\mathcal{L}_{odd}$ denote the set of odd Lucas divisors and $\mathcal{L}$ the set of Lucas divisors. We first show that

$$\mathcal{L}_{odd}(x) = \frac{x}{\log x}(\sum_{j=0}^{t-1} d_j \log^{\delta_{j+1}} x + O(\log^{\delta_{t+1}} x)), \tag{18}$$

with $d_0, \cdots, d_{t-1}$ positive constants. From this it is then deduced that a similar estimate holds for $\mathcal{L}(x)$, with different constants d_j. This then finishes the proof of

Theorem 1.

By Theorem 2,

$$\mathcal{L}_{odd} = \bigcup_{r=1}^{\infty} G_r,$$

where G_r is the set of natural numbers including 1 which are composed of primes in C_r only. The sets G_r are completely multiplicative; $ab \in G_r$ if and only if $a, b \in G_r$, where a and b are natural numbers. Furthermore $G_r \cap G_s = \{1\}$ for $r \neq s$. Thus the problem of estimating $\mathcal{L}_{odd}(x)$, and, as we will see, that of estimating $\mathcal{L}(x)$, reduces to that of estimating $G_r(x)$ for $r \geq 1$. In order to estimate $G_r(x)$, we use the following estimate:

Theorem 6 [9] *Let S be a completely multiplicative set of natural numbers such that*

$$\sum_{p \in S,\ p \leq x} 1 = \tau \mathrm{Li}(x) + O(\frac{x(\log\log x)^g}{\log^3 x}), \tag{19}$$

where $\tau > 0$ and $g \geq 0$ are fixed. Then

$$S(x) = cx \log^{\tau-1} x + O(x(\log\log x)^{g+1} \log^{\tau-2} x),$$

where $c > 0$ is a constant.

(In order to prove Theorem 1 this result is stronger than necessary. The weaker result [13, Theorem 2], for example, will do.) By Theorem 3 the estimate (19) is satisfied with $S = G_r$, $\tau = \delta_r$ and $g = 4$. Applying Theorem 6 and using $\delta_r \leq \frac{1}{3}$, we obtain

$$G_r(x) = d_r x \log^{\delta_r - 1} x + O(x \log^{\delta_{t+1}-1} x), \tag{20}$$

for some positive constant d_r. The estimate (18) for $\mathcal{L}_{odd}(x)$ now follows once we show that

$$\sum_{r=t+1}^{\infty} G_r(x) = O(x \log^{\delta_{t+1}-1} x). \tag{21}$$

To this end, notice that the primes in C_r, $r \geq s \geq 1$, satisfy $p \equiv \pm 1 (\mathrm{mod}\ 2^s)$. Thus

$$\sum_{r \geq s} G_r(x) \leq \sum_{\substack{n \leq x \\ p|n \Rightarrow p \equiv \pm 1 (\mathrm{mod}\ 2^s)}} 1.$$

This latter sum can be estimated with the help of Theorem 6 and the estimate

$$\pi(x; 2^s, 1) := \sum_{\substack{p \leq x \\ p \equiv \pm 1 (\mathrm{mod}\ 2^s)}} 1 = \frac{2}{2^{s-1}} \mathrm{Li}(x) + O(\frac{x}{\log^3 x}),$$

which follows from the prime number theorem for arithmetic progressions. Thus by choosing s large enough (taking $2^{s-2} \geq 1/\delta_{t+1}$ will do), we can ensure that $\sum_{r \geq s} G_r(x) = O(x \log^{\delta_{t+1}-1} x)$. By (20) and the fact that $\{\delta_r\}_{r=1}^{\infty}$ is monotonic decreasing, we have

$$\sum_{t+1 \leq r \leq s} G_r(x) = O(x \log^{\delta_{t+1}-1} x).$$

Thus (21) holds and (18) follows.

It remains to deal with even Lucas divisors. Note that $2\|L_n$ iff $n \equiv 0(\text{mod } 6)$, that $4\|L_n$ iff $n \equiv 3(\text{mod } 6)$ and that 8 is not a Lucas divisor. Suppose m is an odd Lucas divisor, say $m|L_n$. Then $2m|L_{6n}$ and so $2m$ is a Lucas divisor, $4m$ is only a Lucas divisor if the rank of apparition of all the prime divisors of m is exactly divisible by 2, finally $8m$ is never a divisor. Thus $\mathcal{L}(x) = \mathcal{L}_{odd}(x) + \mathcal{L}_{odd}(\frac{x}{2}) + G_1(\frac{x}{4})$. Theorem 1 follows on invoking the estimate (18) and (20) with $r = 1$. □

Remark. Let $h \geq 1$ be an integer. Let $\mathcal{L}_h$ denote the set of divisors of $\{L_{hn}\}_{n=0}^{\infty}$. It is possible to formulate and prove an analogue of Theorem 1 for $\mathcal{L}_h(x)$.

The rank of apparition of p in the
Fibonacci sequence is denoted by $\rho(p)$.

Table 1

Prime density of the set
$\{p : p \equiv \pm 1 (\mathrm{mod}\ 5),\ p \equiv 1 + 2^j (\mathrm{mod}\ 2^{j+1}),\ 2^e \| \rho(p)\}$

$e \backslash j$	1	2	3	4	5	6	7	...	
0	0	$\frac{1}{16}$	$\frac{1}{64}$	$\frac{1}{256}$	$\frac{1}{1024}$	$\frac{1}{4096}$	$\frac{1}{16384}$	..	$\frac{1}{12}$
1	$\frac{1}{4}$	$\frac{1}{16}$	$\frac{1}{64}$	$\frac{1}{256}$	$\frac{1}{1024}$	$\frac{1}{4096}$	$\frac{1}{16384}$	..	$\frac{1}{3}$
2	0	0	$\frac{1}{32}$	$\frac{1}{128}$	$\frac{1}{512}$	$\frac{1}{2048}$	$\frac{1}{8192}$	...	$\frac{1}{24}$
3	0	0	0	$\frac{1}{64}$	$\frac{1}{256}$	$\frac{1}{1024}$	$\frac{1}{4096}$	...	$\frac{1}{48}$
4	0	0	0	0	$\frac{1}{128}$	$\frac{1}{512}$	$\frac{1}{2048}$	...	$\frac{1}{96}$
5	0	0	0	0	0	$\frac{1}{256}$	$\frac{1}{1024}$	...	$\frac{1}{192}$
6	0	0	0	0	0	0	$\frac{1}{512}$	...	$\frac{1}{384}$
...	...	...	...	...	...	...	...	...	...
	$\frac{1}{4}$	$\frac{1}{8}$	$\frac{1}{16}$	$\frac{1}{32}$	$\frac{1}{64}$	$\frac{1}{128}$	$\frac{1}{256}$	...	$\frac{1}{2}$

Table 2

Prime density of the set
$\{p : p \equiv \pm 2 (\mathrm{mod}\ 5),\ p \equiv -1 + 2^j (\mathrm{mod}\ 2^{j+1}),\ 2^e \| \rho(p)\}$

$e \backslash j$	1	2	3	4	5	6	7	...	
0	$\frac{1}{4}$	0	0	0	0	0	0	...	$\frac{1}{4}$
1	0	0	0	0	0	0	0	...	0
2	0	$\frac{1}{8}$	0	0	0	0	0	...	$\frac{1}{8}$
3	0	0	$\frac{1}{16}$	0	0	0	0	...	$\frac{1}{16}$
4	0	0	0	$\frac{1}{32}$	0	0	0	...	$\frac{1}{32}$
5	0	0	0	0	$\frac{1}{64}$	0	0	...	$\frac{1}{64}$
6	0	0	0	0	0	$\frac{1}{128}$	0	...	$\frac{1}{128}$
...	...	...	...	...	...	...	...	...	...
	$\frac{1}{4}$	$\frac{1}{8}$	$\frac{1}{16}$	$\frac{1}{32}$	$\frac{1}{64}$	$\frac{1}{128}$	$\frac{1}{256}$	...	$\frac{1}{2}$

References

[1] C. Ballot, Density of prime divisors of linear recurrences, *Mem. of the Amer. Math. Soc.* **551**, 1995.

[2] J. W. S. Cassels and A. Fröhlich (Eds.), *Algebraic number theory*, Academic Press, London, 1967.

[3] P. D. T. A. Elliott, A problem of Erdös concerning power residue sums, *Acta Arithmetica* **13** (1967), 131-149.

[4] P. D. T. A. Elliott, On the mean value of $f(p)$, *Proc. London Math. Soc.* **21** (1970), 28-96.

[5] H. Hasse, Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerader bzw., ungerader Ordnung mod. p ist, *Math. Ann.* **166** (1966), 19-23.

[6] H. Hasse, *Vorlesungen über Klassenkörpertheorie*, Physica-Verlag, Würzburg, 1967.

[7] J. C. Lagarias, The set of primes dividing the Lucas numbers has density 2/3, *Pacific J. Math.* **118** (1985), 449-461 (Errata, *Pacific J. Math.* **162** (1994), 393-397).

[8] E. Landau, Über Ideale und Primideale in Idealklassen, *Math. Z.* **2** (1918), 52-154.

[9] P. Moree, On the divisors of $a^k + b^k$, MPI-preprint 130, 1995.

[10] B. Z. Moroz, Scalar product of Hecke L-functions and its application, *Zeta functions in geometry*, Advanced studies in pure mathematics **21** (1992), 153-171.

[11] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Springer-Verlag, Berlin, 1990.

[12] R. W. K. Odoni, A conjecture of Krishnamurty on decimal periods and some allied problems, *J. Number Theory* **13** (1981), 303-319.

[13] R. W. K. Odoni, A problem of Rankin on sums of powers of cusp-form coefficients, *J. London Math. Soc.* **44** (1991), 203-217.

[14] V. Pless, P. Solé and Z. Qian, Cyclic self dual $\mathbb{Z}_4$-codes and type I lattices, preprint.

[15] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Cambridge University Press, Cambridge, 1989.

[16] P. J. Stephens, Prime divisors of second order linear recurrences I, *J. Number Theory* **8** (1976), 313-332.

[17] M. Ward, Prime divisors of second order recurring sequences, *Duke Math. J.* **21** (1954), 607-614.

[18] K. Wiertelak, On the density of some sets of primes. I, II, *Acta Arith.* **34** (1977/78), 183-196, 197-210.

[19] K. Wiertelak, On the density of some sets of primes. III, *Funct. Approx. Comment. Math.* **10** (1981), 93-103.

[20] K. Wiertelak, On the density of some sets of primes. IV, *Acta Arith.* **43** (1984), 177-190.

[21] K. Wiertelak, On the density of some sets of integers, *Funct. Approx. Comment. Math.* **19** (1990), 71-76.

[22] K. Wiertelak, On the density of some sets of primes p, for which $\mathrm{ord}_p(n) = d$. *Funct. Approx. Comment. Math.* **21** (1992), 69-73.

Max-Planck-Institut für Mathematik
Gottfried-Claren Str. 26
53225 Bonn
Germany
Email: morec@antigone.mpim-bonn.mpg.de