PACIFIC JOURNAL OF MATHEMATICS
Vol. 186, No. 2, 1998

COUNTING DIVISORS OF LUCAS NUMBERS

Pieter Moree

The Lucas numbers L_n are defined by $L_0 = 2$, $L_1 = 1$ and the recurrence $L_n = L_{n-1} + L_{n-2}$. An estimate for the number of $m \leq x$ such that m divides some Lucas number is established. This estimate has error of order $x \log^{\epsilon-1} x$ for every $\epsilon > 0$.

1. Introduction.

Let $\{S_n\}$ be a second order linear recurrence consisting of integers only. M. Ward [22] proved that, except for some degenerate cases, there are always an infinite number of distinct primes dividing the terms of $\{S_n\}$. A deeper question is whether in the non-degenerate case the set of prime divisors has a 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.) It is conjectured that the answer is yes and that the density is in fact positive. In case of what are called torsion sequences, this was recently established by P. Stevenhagen [21], generalizing on results in the earlier papers [9, 11, 13]. Stevenhagen showed, moreover, that the density of a torsion sequence is a rational number. For a large class of non-torsion sequences, the existence and positivity of of the prime density was established by P.J. Stephens [20], under the assumption of the Generalized Riemann Hypothesis.

The sequence $\{L_n\}$ is torsion. Lagarias established that it has prime density 2/3. His method goes back to H. Hasse [6], 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 [24, 25, 26, 27, 28]. For a survey of results on prime divisors of, not necessarily second order, linear recurrences, see Ballot [1].

The problem of general divisors of second order linear recurrence sequences, in contrast, has not received much attention. Let a and b be fixed coprime integers such that $|a| \neq |b|$. In [12] the set of divisors, $G_{a,b}$, of the sequence $\{a^k + b^k\}$ was considered. Some of the results obtained there have

an application in coding theory [8, 17]. It was shown that for given $t \geq 1$,

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

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. In contrast the constants $c_0', \cdots, c_t'$ seem to be very difficult to compute.

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 $t \geq 1$,*

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

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

The sequence of exponents $\{2^{-j}/3\}_{j=0}^{\infty}$ appearing in (2) coincides with that appearing in (1) in case $a/b \notin \{\pm\mathbb{Q}^2, \pm 2\mathbb{Q}^2\}$ [12].

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

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

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 [9] only computed δ_0; it equals 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.

A natural question that arises is whether Theorem 1 can be extended to other sequences of the form $\{\alpha^n + \bar{\alpha}^n\}_{n=0}^{\infty}$ with α an algebraic integer from a quadratic field $\mathbb{Q}(\sqrt{D})$. In the case $D > 0$ and α is a unit this certainly seems to be the case. Since the exponents in (2) depend in an idiosyncratic way on α, it will be awkward to state and prove a generalization of Theorem 1 of this type. I have restricted myself therefore to the most well-known of the sequences of the above form. Given the necessary patience the reader should be able to work out some other cases as well. It is not clear what to expect for general second-order linear recurrences. Then both Theorem 2 and the Hasse method fail.

I would like to thank K. Belabas, B. Moroz, G. Niklasch and P. Stevenhagen for helpful (e-mail) discussions. The comments of Stevenhagen on an earlier version allowed me to shorten some of the proofs.

2. Characterization of Lucas divisors.

The following properties of the Fibonacci and Lucas number are well-known (see e.g. [18, pp. 41-55]):

(i) $m|F_n$ if and only if $\rho(m)|n$;
(ii) If $p|F_n$, then $p^e|F_{np^{e-1}}$ for $e \geq 1$;
(iii) $L_nF_n = F_{2n}$;
(iv) $(F_n, L_n)|2$;
(v) If $b \geq 1$ and odd, then $L_a|L_{ab}$.

These properties will be used to derive a characterization of divisors of Lucas numbers. To this end we need a proposition and a lemma.

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

Proof. By (i) and (ii) it follows that $\rho(p^r)|\rho(p)p^{r-1}$. Clearly $\rho(p)|\rho(p^r)$. Thus the proposition follows. □

Lemma 1. *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*

$$p^r|L_n \iff n \equiv \frac{\rho(p^r)}{2} (\text{mod } \rho(p^r)). \tag{4}$$

Proof. We prove the first part of the assertion. The proof of the second part is similar and left to the reader. Let p^r be odd. If it divides L_n, then by (iii) it divides F_{2n} and thus by (i) $2n \equiv 0 (\mathrm{mod}\ \rho(p^r))$. If $\rho(p^r)$ would be odd then p^r would divide F_n, thus contradicting (iv). Suppose $\rho(p^r)$ is even. Then $L_{\frac{\rho(p^r)}{2}} F_{\frac{\rho(p^r)}{2}} = F_{\rho(p^r)}$. Using (i) and (iv) it then follows that $p^r | L_{\frac{\rho(p^r)}{2}}$. □

Using this result it is not difficult to prove the following result characterizing odd divisors of Lucas numbers.

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. Let $m = \prod_{i=1}^{s} p_i^{e_i}$ be the canonical prime factorization of m.

'⇒'. By Lemma 1 it follows there exist odd integers b_i such that

$$\frac{\rho(p_1^{e_1})}{2} b_1 = \cdots = \frac{\rho(p_s^{e_s})}{2} b_s.$$

Thus there exists $e \geq 1$ such that $2^e || \rho(p^r)$ for all prime powers p^r dividing m. By Proposition 1 this implies there exists $e \geq 1$ such that $2^e || \rho(p)$ holds for all primes p dividing m.

'⇐'. Put $a_i = \rho(p_i)/2^e$, $1 \leq i \leq s$. Then a_i is odd. Using (4) and Proposition 1, we see that $m | L_{2^{e-1} m a_1 \cdots a_s}$. □

The behaviour of $\{F_n\}$ and $\{L_n\}$ is intimately connected with certain aspects of the arithmetic of $\mathbb{Q}(\sqrt{5})$. In the remainder of this section we will deal with some elementary aspects of this connection that will be needed in the sequel.

Put $\epsilon = (1+\sqrt{5})/2$, $\bar{\epsilon} = (1-\sqrt{5})/2$, $\theta = \epsilon/\bar{\epsilon}$. Note that $\theta = -\epsilon^2 = -(3+\sqrt{5})/2$. 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

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

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 divides some non-zero Fibonacci number if and only if for some $x \geq 1$ the congruence $\theta^x \equiv 1 (\mathrm{mod}\ (m))$ holds in $\mathbb{Z}[\epsilon]$. 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 $p \neq 5$, $r \geq 1$,

$$p^r | L_n \iff \theta^n \equiv -1 (\mathrm{mod}\ (p^r)) \iff \theta^n \equiv -1 (\mathrm{mod}\ \mathfrak{P}^r), \tag{5}$$

where $\mathfrak{P}$ is any prime ideal dividing (p). The second equivalence in (5) follows on noting that $\theta^n + 1$ is a unit times a rational integer and so $\mathfrak{P}^r$ divides $\theta^n + 1$ if and only if (p^r) does.

Lemma 2. *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 $\mathbb{Z}[\epsilon]/\mathfrak{P} \cong \mathbb{F}_{p^2}$. Then $\theta^p \equiv \bar{\theta} (\mathrm{mod}\ \mathfrak{P})$ and so $1 = N(\theta) = \theta \cdot \bar{\theta} \equiv \theta^{p+1} (\mathrm{mod}\ \mathfrak{P})$. Therefore $\mathrm{ord}_{\mathfrak{P}}(\theta)|p+1$. □

3. Computing the densities δ_e.

In order to prove the estimate (3) we need to compute, for $e \geq 0$, 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 $s = 1, 2,\ e \geq 0,\ j \geq 1$ put

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

Then it follows on noting that $\rho(5) = 5$ 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 $e \geq 1$. 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 [**6**] and was used by several subsequent authors [**1**, **9**, **11**, **13**, **15**, **24**]. 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 $K_{0,n} := \mathbb{Q}(\sqrt{5}, \zeta_{2^n}),\ n \geq 1$, is needed. $K_{0,n}$ is normal over $\mathbb{Q}$ and is easily seen to be of degree 2^n over $\mathbb{Q}$. As compositum of the abelian fields $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\zeta_{2^n})$, $K_{0,n}$ is abelian. 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. Since 5 does not ramify in $\mathbb{Q}(\zeta_{2^n})$ we have $d_{K_{0,n}/\mathbb{Q}(\zeta_{2^n})} = (5)$. Now if $K \subseteq L \subseteq M$ is a tower of fields, then (see e.g. [**14**, Proposition 4.9])

$$d_{M/K} = (N_{L/K} d_{M/L}) d_{L/K}^{[M:L]}. \tag{6}$$

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 $p \equiv \pm 1 (\mathrm{mod}\ 5)$ and $p \equiv 1 (\mathrm{mod}\ 2^n)$.

For $b \geq a$ put $K_{a,b} = \mathbb{Q}(\sqrt{5}, \theta^{1/2^a}, \zeta_{2^b})$ and $d_{a,b} = [K_{a,b} : \mathbb{Q}]$.

Lemma 3. *For $b > a \geq 1$, $d_{a,b} = 2^{a+b-1}$. Furthermore $d_{0,b} = 2^b$, $b \geq 1$, $d_{1,1} = 4$ and $d_{b,b} = 2^{2b-1}$ for $b \geq 2$.*

Proof. When $b > a \geq 1$, $K_{a,b} = \mathbb{Q}(\sqrt{5}, \epsilon^{1/2^{a-1}}\zeta_{2^{a+1}}, \zeta_{2^b}) = \mathbb{Q}(\epsilon^{1/2^{a-1}}, \zeta_{2^b})$. I claim that $X^{2^{a-1}} - \epsilon$ is irreducible over $K_{0,b}$, for if it were not, then $\mathbb{Q}(\sqrt{\epsilon})$ would be a subfield of the abelian field $K_{0,b}$ and hence normal. However, by [5, Satz 1], $\mathbb{Q}(\sqrt{\epsilon})$ is not normal. Thus $X^{2^{a-1}} - \epsilon$ is irreducible over $K_{0,b}$ and hence $d_{a,b} = 2^{a-1}d_{0,b} = 2^{a+b-1}$. The degrees $d_{b,b}$ were computed in [9, Lemma 3.1]. □

Lemma 4. *A prime p satisfies*

$$p \equiv \pm 1 (\mathrm{mod}\ 5),\ p \equiv 1 + 2^j (\mathrm{mod}\ 2^{j+1}),\ \theta^{\frac{p-1}{2^t}} \equiv 1 (\mathrm{mod}\ \mathfrak{P}), \tag{7}$$

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 (7) equals $1/d_{t,j} - 1/d_{t,j+1}$.

Proof. The proof of the last part of the assertion follows from the first part and the Chebotarev density theorem. Note that it is enough to show that for $j \geq 1$, $t \leq j$, the primes p for which $p \equiv \pm 1 (\mathrm{mod}\ 5)$, $p \equiv 1 (\mathrm{mod}\ 2^j)$, $\theta^{\frac{p-1}{2^t}} \equiv 1 (\mathrm{mod}\ \mathfrak{P})$ are precisely those that split completely in $K_{t,j}$. The primes satisfying $p \equiv \pm 1 (\mathrm{mod}\ 5)$, $p \equiv 1 (\mathrm{mod}\ 2^j)$ are precisely those that split completely in $K_{0,j}$. Now let p be a prime that splits completely in $K_{0,j}$. Note that p is odd. Then $\theta^{\frac{p-1}{2^t}} \equiv 1 (\mathrm{mod}\ \mathfrak{P})$ implies by Euler's criterion that $X^{2^t} \equiv \theta (\mathrm{mod}\ \mathfrak{P})$ has a solution in $\mathbb{Z}[\epsilon]$. Let $\mathfrak{Q}$ be a prime ideal of $\mathfrak{O}_{K_{o,j}}$ 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 in $\mathbb{Z}[\epsilon]$ iff

$$X^{2^t} \equiv \theta (\mathrm{mod}\ \mathfrak{Q}) \tag{8}$$

has a solution in $\mathfrak{O}_{K_{0,j}}$. Thus the proof will be completed once we show that $\mathfrak{Q}$ splits completely in $K_{t,j}/K_{0,j}$ iff (8) has a solution in $\mathfrak{O}_{K_{0,j}}$. So assume (8) has such a solution. Since $\zeta_{2^t} \in \mathfrak{O}_{K_{0,j}}$ and $\mathfrak{Q}$ does not extend 2, the latter congruence has 2^t distinct solutions. Let $f(X)$ be a monic irreducible polynomial over $K_{0,j}$ such that $f(X)|X^{2^t} - \theta$ and $K_{0,j}(X)/(f(X)) \cong K_{t,j}$. It now follows by [16, Example 29] that in $\mathfrak{O}_{K_{0,j}}$ we have $\mathfrak{Q} = \mathfrak{P}_1 \cdots \mathfrak{P}_s$, where $s = [K_{t,j} : K_{0,j}]$ and the prime ideals $\mathfrak{P}_\nu$ are pairwise distinct. Thus $\mathfrak{Q}$ splits completely in $K_{t,j}/K_{0,j}$. If (8) does not have a solution in $\mathfrak{O}_{K_{0,j}}$ it follows similarly that $\mathfrak{Q}$ decomposes in $K_{t,j}$ as a product of prime ideals of residual degree at least 2. □

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 5. *$\Delta_1(e,j)=0$ 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 (5) the assertion $2^e\|\mathrm{ord}_{(p)}(\theta)$ is equivalent with

$$2^e\|\mathrm{ord}_{\mathfrak{P}}(\theta), \tag{9}$$

where $\mathfrak{P}|(p)$. That $\Delta_1(e,j)=0$ for $e>j$ is immediate by Lemma 2. So assume $e\leq j$. In case $e=0$ the condition (9) is equivalent with $\theta^{\frac{p-1}{2^j}}\equiv 1(\mathrm{mod}\ \mathfrak{P})$. Then, by Lemma 4, $\Delta_1(0,j)=1/d_{j,j}-1/d_{j,j+1}$. Using Lemma 3 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 (9) 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 4, 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 3. □

The case $s=2$. Let $p\equiv\pm 2(\mathrm{mod}\ 5)$. Recall that $\mathrm{ord}_{(p)}(\theta)|p+1$. Since $\epsilon\bar{\epsilon}=-1$ and $\epsilon^p\equiv\bar{\epsilon}(\mathrm{mod}\ (p))$, $\epsilon^{p+1}\equiv -1(\mathrm{mod}\ (p))$. 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 we have $2^j\|\mathrm{ord}_{(p)}(\theta)$ 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 it follows that $\Delta_2(j,j)=1/2^{j+1}$ and $\Delta_2(e,j)=0$ whenever $e\neq j$. In case $j=1$ and $p\equiv 1(\mathrm{mod}\ 4)$ we have $\theta^{\frac{p+1}{2}}=(-1)^{\frac{p+1}{2}}\epsilon^{p+1}\equiv 1(\mathrm{mod}\ (p))$. Thus, using that $(p+1)/2$ is odd, we find $N_2(0,1)=\{p: p\equiv\pm 2(\mathrm{mod}\ 5), p\equiv 1(\mathrm{mod}\ 4)\}$, $\Delta_2(0,1)=1/4$ 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 the density δ_e satisfies $\delta_e=\sum_{j=1}^{\infty}\{\Delta_1(e,j)+\Delta_2(e,j)\}$. 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 [**26**], 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 [**15**], 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*

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

where $\delta_0 = 1/3$, $\delta_e = 2^{1-e}/3$ 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 [9, Theorem B]:

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

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

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

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 [10]). 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 $N_{K/\mathbb{Q}}\mathfrak{A}$, the absolute 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 6 ([26])**.** *Let K be a number field. There exists an absolute positive constant g_1 such that*

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

where

$$R = \frac{x\log(2\Delta)}{\sqrt{\log x}} \exp\left(-g_1 \frac{\log x}{\max\{\sqrt{[K:\mathbb{Q}]\log x}, \log\Delta\}}\right).$$

Reasoning as in [19], see especially page 148, we find (cf. [26, Lemma 5.2]):

Lemma 7. *Let K be normal over $\mathbb{Q}$. Then there exists an absolute constant $c_1 > 0$ such that*

$$\beta_1 < \max\left(1 - \frac{1}{4\log\Delta}, 1 - \frac{c_1}{\Delta^{1/[K:\mathbb{Q}]}}\right).$$

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 $\left(\frac{\psi}{\mathfrak{P}}\right)_m \equiv \psi^{\frac{N\mathfrak{P}-1}{m}} \pmod{\mathfrak{P}}$. 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 8. *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 $(4m^2\alpha)$ and $\mathfrak{B}'\mathfrak{B}^{-1} = (c)$, where c is totally positive and $c \equiv 1((4m^2\alpha))$, 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 [7, 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 the extension $K(\zeta_m, \alpha^{1/m})$ of $K(\zeta_m)$ (see e.g. [2, p. 273]). The proof then follows on using an estimate due to Hasse for the conductor of Kummerian fields ([7, Satz 166]; the meaning of the symbols ν and s_0 appearing in Satz 166 is explained in Satz 164). □

Lemma 8 was proved in case $K = \mathbb{Q}$ by Elliott [4] with $4m^2\alpha$ replaced by $m^2\alpha$. Elliott made heavy use of classical reciprocity results due to Hasse. The point of Lemma 8 is that it shows that the conductor of $K(\zeta_m, \alpha^{1/m})$, viewed as a function of m, is polynomial in m, rather than superexponential, which would follow on estimating the conductor by the discriminant. Using the superexponential 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 $\hat{\pi}_M(x)$ 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*

$$\hat{\pi}_M(x) = \frac{\mathrm{Li}(x)}{[M:\mathbb{Q}]} + O\left(\frac{x}{\log^C x}\right),$$

uniformly for

$$2^n \le g_2 \frac{\log x}{(\log\log x)^2},\ r \le n. \tag{10}$$

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

Proof of Theorem 5. Put $L = K(\zeta_{2^n})$ and $M = L(\psi^{1/2^r})$. 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 $r \le n$. Let S_M denote the set of rational primes p such that $(p, 2N_{K/\mathbb{Q}}(\psi)) = 1$, p splits completely in L and $X^{2^r} \equiv \psi (\mathrm{mod}\ \mathfrak{P})$, where $\mathfrak{P}$ is any prime ideal dividing (p), has a solution in $\mathfrak{O}_L$. Reasoning as in the proof of Lemma 4 we find

$$\hat{\pi}_M(x) = S_M(x) + O(1). \tag{11}$$

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

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

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

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

Now let us define $T_{M,1} = \left\{\mathfrak{P} : (\mathfrak{P}, 2^n\psi) = 1,\ \left(\frac{\psi}{\mathfrak{P}}\right)_{2^r} = 1,\ f(\mathfrak{P}|p) = 1\right\}$ and $T_M = \left\{\mathfrak{P} : (\mathfrak{P}, 2^n\psi) = 1,\ \left(\frac{\psi}{\mathfrak{P}}\right)_{2^r} = 1\right\}$. 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

$$S_M(x) = \frac{T_M(x)}{[L : \mathbb{Q}]} + O(\sqrt{x}\log x). \tag{12}$$

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

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

Thus we can write

$$T_M(x) = \sum_{N\mathfrak{P}\le x,\ \left(\frac{\psi}{\mathfrak{P}}\right)_{2^r}=1} 1 = \frac{1}{2^r}\sum_{j=1}^{2^r}\sum_{N\mathfrak{P}\le x}\left(\frac{\psi^j}{\mathfrak{P}}\right)_{2^r}, \tag{13}$$

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 $(\mathfrak{A}, 4^{n+1}\psi) = 1$ and zero otherwise. By the multiplicativity of χ_j and Lemma

8, χ_j is a character of the group of ideal classes modulo $(4^{n+1}\psi)$, the principal ideal in $\mathfrak{O}_L$ generated by $4^{n+1}\psi$. Thus we can rewrite (13) as

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

From this, Lemma 6, (12) and (11) we obtain

$$\hat{\pi}_M(x) = \frac{a_M}{[L:\mathbb{Q}]}\mathrm{Li}(x) - \frac{b_M}{[L:\mathbb{Q}]}\mathrm{Li}(x^{\beta_1}) + O(R) + O(\sqrt{x}\log x), \tag{14}$$

with $0 \le a_M, b_M \le 1$, R as in Lemma 6 and $\Delta = |d_{L/\mathbb{Q}}| \cdot N_{L/\mathbb{Q}}(8^n\psi)$. We have $\log\Delta \le g_3 2^n n$, where g_3 depends at most on ψ and K. If r and n satisfy (10) then

$$\log\Delta \le g_2 g_3 \frac{\log x}{\log\log x}, \tag{15}$$

where g_2 is still to be chosen. Let $C > 0$ be given. Using the estimate (15) and Lemma 7 to deal with the exceptional zero β_1 in (14), we see that we can choose g_2 so small as to ensure that $\hat{\pi}_M(x) = a_M\mathrm{Li}(x)/[L:\mathbb{Q}] + O(x\log^{-C}x)$ uniformly in the region (10). 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. [**15**]). 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 with $K = \mathbb{Q}(\sqrt{5})$ and $\psi = \theta = -(3+\sqrt{5})/2$, we find using Lemma 4 that there exists an absolute positive constant g_4 such that uniformly for $2^j \le g_4\log x(\log\log x)^{-2}$, $e \le j$,

$$N_1(e,j)(x) = \Delta_1(e,j)\mathrm{Li}(x) + O\left(\frac{x}{\log^3 x}\right) \tag{16}$$

(cf. the proof of Lemma 5). 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 $2^m \le g_4\log x(\log\log x)^{-2}$. Using equation (16) and

$\Delta_1(e,j) \ll 1/4^j$ (see Lemma 5) we find

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

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 $I_2(x) \le \hat{\pi}_{K_{m,m}}(x)$ (cf. the proof of Lemma 4). By Lemma 3 $[K_{m,m} : \mathbb{Q}] \gg 4^m$. It follows from this estimate, Theorem 5 and $2^m \le g_4 \log x(\log\log x)^{-2}$ that $I_2(x) = O(x(\log\log x)^4 \log^{-3} x)$. Thus

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

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

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

Thus

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

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 $\delta_j = 2^{1-j}/3$, $j \ge 1$. Let $\mathcal{L}_{\mathrm{odd}}$ denote the set of odd Lucas divisors and $\mathcal{L}$ the set of Lucas divisors.

We first show that

$$\mathcal{L}_{\text{odd}}(x) = \frac{x}{\log x}\left(\sum_{j=0}^{t-1} d_j \log^{\delta_{j+1}} x + O(\log^{\delta_{t+1}} x)\right), \tag{17}$$

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,

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

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 $\mathcal{L}_{\text{odd}}(x)$, 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 ([12]). *Let S be a completely multiplicative set of natural numbers such that*

$$\sum_{p \in S,\ p \leq x} 1 = \tau \text{Li}(x) + O\left(\frac{x(\log\log x)^g}{\log^3 x}\right), \tag{18}$$

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.

For $S = G_r$ (18) is satisfied with $\tau = \delta_r$ and $g = 4$ by Theorem 3. Applying Theorem 6 and using $\delta_r \leq \frac{1}{3}$, we obtain

$$G_r(x) = d_r x \log^{\delta_r - 1} x + O\left(x \log^{\delta_{t+1} - 1} x\right), \tag{19}$$

for some positive constant d_r. The estimate (17) for $\mathcal{L}_{\text{odd}}(x)$ now follows once we show that

$$\sum_{r=t+1}^{\infty} G_r(x) = O\left(x \log^{\delta_{t+1} - 1} x\right). \tag{20}$$

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

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

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

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

which follows from the prime number theorem for arithmetic progressions. Thus by choosing s large enough (taking $2^{s-2} \ge 1/\delta_{t+1}$ will do), we can ensure that $\sum_{r\ge s} G_r(x) = O\left(x\log^{\delta_{t+1}-1} x\right)$. By (19) and the fact that $\{\delta_r\}_{r=1}^{\infty}$ is monotonic decreasing, we have

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

Thus (20) holds and (17) follows.

It remains to deal with even Lucas divisors. Note that $2\|L_n$ iff $n \equiv 0(\mathrm{mod}\ 6)$, that $4\|L_n$ iff $n \equiv 3(\mathrm{mod}\ 6)$ 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 $\rho(p)$ of all the prime divisors p of m is exactly divisible by 2, finally $8m$ is never a divisor. Thus $\mathcal{L}(x) = \mathcal{L}_{\mathrm{odd}}(x) + \mathcal{L}_{\mathrm{odd}}(\frac{x}{2}) + G_1(\frac{x}{4})$. Theorem 1 follows on invoking the estimate (17) and (19) with $r = 1$.

Remark. Let $h \ge 1$ 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 $\mathcal{L}_h(x)$.

6. Explicit divisibility criteria.

Table 1 and 2 can be used to derive some explicit criteria for primes to divide Lucas numbers. We leave it to the reader to prove that if an entry in one of the tables is zero, then the corresponding set is empty. Using Table 1 and 2 it then follows that p is a divisor of $\{L_n\}$ if $p \equiv 3(\mathrm{mod}\ 4)$; that is if $p \equiv 3, 7, 11, 19(\mathrm{mod}\ 20)$, p is a non-divisor of $\{L_n\}$ if $p \equiv 13, 17(\mathrm{mod}\ 20)$. This is Lemma 2.1 of [**23**]. More in particular we have $p \in C_0$ if $p \equiv 13, 17(\mathrm{mod}\ 20)$, $p \in C_1$ if $p \equiv 11, 19(\mathrm{mod}\ 20)$ and $p \in C_{\mathrm{ord}_2(p+1)}$ if $p \equiv 3, 7(\mathrm{mod}\ 20)$. The primes $p \equiv 1, 9(\mathrm{mod}\ 20)$ are not covered. By Table 1 the primes $p \equiv 21, 29(\mathrm{mod}\ 40)$ are either in C_0 or in C_1. Each such prime is represented by the form $X^2 + 4Y^2$. Let $(X, Y) = (u, v)$ be such a representation. Then $p \in C_1$ if and only if $u \equiv \pm 1(\mathrm{mod}\ 5)$ or $v \equiv \pm 1(\mathrm{mod}\ 5)$. This follows using a result of Ward [**23**, Theorem 3.3]. Thus 7/8th of all primes are covered. Similar results can be proved for the recurrences $\{a^k + b^k\}$ (see [**12**, Section 6]).

Using the fact that the second row in Table 2 has only zero entries it is deduced that the Lucas number L_n with $n \equiv 1(\mathrm{mod}\ 2)$ is composed only of

primes p satisfying $p = 2$ or $p \equiv \pm 1 (\mathrm{mod}\ 5)$. In fact the number of divisors m of $\{L_{1+2n}\}$ not exceeding x equals

$$c\frac{x}{\log^{2/3} x} + O\left(x\frac{(\log\log x)^5}{\log^{5/3} x}\right),$$

where $c > 0$. This estimate is quite different from that for the sequence $\{L_{2n}\}$ (cf. the final remark of Section 5).

The rank of apparition of the prime 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), 102.

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

[3] P.D.T.A. Elliott, *The distribution of power residues and certain related results*, Acta Arithmetica, **17** (1970), 141-159.

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

[5] F. Halter-Koch, *Arithmetische theorie der Normalkörper von 2-potenzgrad mit diedergruppe*, J. Number Theory, **3** (1971), 412-443.

[6] 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.

[7] ———, *Vorlesungen über klassenkörpertheorie*, Physica-Verlag, Würzburg, 1967.

[8] P. Kanwar and S. López-Permouth, *Cyclic codes over the integers modulo p^m*, Finite Fields Applic., **3** (1997), 334-352.

[9] 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).

[10] E. Landau, *Über ideale und primideale in idealklassen*, Math. Z., **2** (1918), 52-154.

[11] P. Moree, *On the prime density of Lucas sequences*, Journal de Théorie des Nombres de Bordeaux, **8** (1996), 449-459.

[12] ———, *On the divisors of $a^k + b^k$*, Acta Arithmetica, **80** (1997), 197-212.

[13] P. Moree and P. Stevenhagen, *Prime densities for Lucas sequences*, Acta Arithmetica, **80** (1997), 403-410.

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

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

[16] A.N. Parshin and I.R. Shafarevich (Eds.), *Number theory* II, Springer-Verlag, Berlin, 1992.

[17] V. Pless, P. Solé and Z. Qian, *Cyclic self dual $\mathbb{Z}_4$-codes*, Finite Fields Applic., **3** (1997), 48-69.

[18] P. Ribenboim, *The book of prime number records*, Springer-Verlag, Berlin, 1988.

[19] H.M. Stark, *Some effective cases of the Brauer-Siegel theorem*, Invent. Math., **23** (1974), 135-152.

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

[21] P. Stevenhagen, *Prime densities for second order torsion sequences*, in preparation.

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

[23] ———, *The prime divisors of Fibonacci numbers*, Pacific J. Math., **11** (1961), 379-386.

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

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

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

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

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

Received June 3, 1997 and revised February 9, 1998.

Max-Planck-Institut für Mathematik
Gottfried-Claren Strasse 26
53225 Bonn, Germany
E-mail address: moree@mpim-bonn.mpg.de

Faculteit WINS
Universiteit van Amsterdam
1018 TV Amsterdam
The Netherlands