ACTA ARITHMETICA
LXXXII.4 (1997)

Prime divisors of Lucas sequences

by

Pieter Moree (Bonn) and Peter Stevenhagen (Amsterdam)

1. Introduction. Let $d > 1$ be a squarefree integer and $K = \mathbb{Q}(\sqrt{d})$ the corresponding real quadratic field. We write $\varepsilon = a + b\sqrt{d}$ for a fundamental unit in the ring of integers of K, and $\overline{\varepsilon}$ for its conjugate. The *Lucas sequence* associated with K is the integer sequence

$$X_K = \{\mathrm{Tr}_{K/\mathbb{Q}}(\varepsilon^n)\}_{n=0}^{\infty} = \{\varepsilon^n + \overline{\varepsilon}^n\}_{n=0}^{\infty}.$$

For odd n the sign of x_n depends on the choice of the sign of a. This is irrelevant for the divisibility properties we will be concerned with, but for uniqueness sake we take $x_1 = 2a > 0$.

The Lucas sequence X_K satisfies the second order linear recurrence

$$x_{n+2} = 2ax_{n+1} - N_{K/\mathbb{Q}}(\varepsilon)x_n$$

for $n \geq 0$. If we take for K the field $\mathbb{Q}(\sqrt{5})$ generated by the golden ratio, we obtain the very classical example of the Lucas sequence defined by the "Fibonacci recursion" $x_{n+2} = x_{n+1} + x_n$ with initial values $x_0 = 2$ and $x_1 = 1$.

In this note, we show that the set of prime numbers p that divide some term of the sequence X_K has a natural density δ_K and determine it for each K. More precisely, we compute the density δ_K^+ of the primes that split completely in K and divide some term of X_K and the density δ_K^- of the primes that are inert in K and divide some term of X_K. The arguments for both kinds of primes are somewhat different, and so are the associated densities. It turns out that the determination of δ_K^- is the more difficult part, unless we are in the "easy case" in which the norm $N_{K/\mathbb{Q}}(\varepsilon)$ equals -1, when it is trivially determined. Clearly, one has $\delta_K = \delta_K^+ + \delta_K^-$.

The method in this note extends to sequences $\{\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^n)\}_{n=0}^{\infty} = \{\alpha^n + \overline{\alpha}^n\}_{n=0}^{\infty}$, where α is any algebraic integer in a quadratic field K. Although it is a bit cumbersome to express the density as an explicit rational number

1991 *Mathematics Subject Classification*: Primary 11R45; Secondary 11B39.
Key words and phrases: Lucas sequence, Chebotarev density theorem.

in terms of α, this yields a proof of what is called a "main conjecture" in [5, p. 362]. For more details, we refer to the treatment of general second order "torsion sequences" in [6].

THEOREM. *Let $K = \mathbb{Q}(\sqrt{d})$ and $a = \frac{1}{2}\operatorname{Tr}_{K/\mathbb{Q}}(\varepsilon) > 0$ be as above. Then the natural densities δ_K^+ and δ_K^- for the sets of prime divisors of the Lucas sequence associated with K exist. For $N_{K/\mathbb{Q}}(\varepsilon) = -1$ the densities are as follows.*

	$d = 2$	$d > 2$
δ_K^+	11/24	5/12
δ_K^-	1/4	1/4
δ_K	17/24	2/3

For $N_{K/\mathbb{Q}}(\varepsilon) = 1$ the densities depend in the following way on whether $a+1$ and $a-1$ are rational squares or not.

	$a-1=\square$	$a+1=\square$	$a\pm 1 \neq \square$
δ_K^+	5/24	5/24	1/6
δ_K^-	1/8	5/24	1/6
δ_K	1/3	5/12	1/3

The main ingredient of the proof is the Chebotarev density theorem, and the basic idea of the method goes back to Hasse [2]. Lagarias [3] was the first to use this idea in a quadratic setting, for the classical Lucas sequence mentioned above, which falls in the category $N_{K/\mathbb{Q}}(\varepsilon) = -1$. A generalization to other instances of units of norm -1 is given in [4]. For the easier and well-studied case of reducible second order recurrences $\{r^n + s^n\}_{n=0}^{\infty}$ with $r, s \in \mathbb{Z}$, or for generalizations to higher order linear recurrences, the reader can consult [1].

2. Proof of the Theorem. Let $K = \mathbb{Q}(\sqrt{d})$ and $\varepsilon = a + b\sqrt{d}$ be as before, and write $\mathcal{O}$ for the ring of integers of K. If p is a prime that is unramified in $K/\mathbb{Q}$, then the kernel of the norm map $\kappa_p = \ker[N : (\mathcal{O}/p\mathcal{O})^* \to \mathbb{F}_p^*]$ is a cyclic group of order $p - \left(\frac{d}{p}\right)$. We set

$$q = q_K = \varepsilon/\overline{\varepsilon} = \begin{cases} -\varepsilon^2 & \text{if } N_{K/\mathbb{Q}}(\varepsilon) = -1, \\ \varepsilon^2 & \text{if } N_{K/\mathbb{Q}}(\varepsilon) = 1. \end{cases} \tag{2.1}$$

Let $p \nmid 2d$ be a prime number. Looking at the explicit form of the nth term $x_n = \varepsilon^n + \overline{\varepsilon}^n$ of X_K, we find that p divides x_n if and only if we have $q^n = -1 \in (\mathcal{O}/p\mathcal{O})^*$. As q lies in the cyclic subgroup $\kappa_p \subset (\mathcal{O}/p\mathcal{O})^*$ and -1 is the unique element of order 2 in that group, we find the basic characterization

$$p \text{ divides some term of } X_K \Leftrightarrow \text{the order of } q \in (\mathcal{O}/p\mathcal{O})^* \text{ is } \textit{even}.$$

The key idea in determining the densities δ_K^+ and δ_K^- is that one can describe the parity of the order of $q \in (\mathcal{O}/p\mathcal{O})^*$ in terms of the splitting behavior of p in some infinite algebraic extension of $\mathbb{Q}$. We start with the easier case of the rational primes that split completely in K.

Split case. Let S^+ be the set of odd primes p that split completely in K, and $D^+ \subset S^+$ the set of primes in S^+ that divide some term of X_K.

For $k \in \mathbb{Z}_{\geq 1}$, we let $S_k^+ \subset S^+$ be the set of primes $p \in S^+$ for which $p-1$ has exactly $k = \mathrm{ord}_2(p-1)$ factors 2. The set S_k^+ consists of the primes that split completely in the field $K(\zeta_{2^k})$ obtained by adjoining to K a primitive 2^kth root of unity, but not in the field $K(\zeta_{2^{k+1}})$ obtained by adjoining to K a primitive 2^{k+1}th root of unity. By the Chebotarev density theorem, the set S_k^+ has a natural density inside the set of all primes. It equals $\delta(S_k^+) = [K(\zeta_{2^k}) : \mathbb{Q}]^{-1} - [K(\zeta_{2^{k+1}}) : \mathbb{Q}]^{-1}$. Clearly, the sum of these densities for all $k \geq 1$ is $[K : \mathbb{Q}]^{-1} = 1/2 = \delta(S^+)$.

For $p \in S_k^+$, the group $(\mathcal{O}/p\mathcal{O})^*$ is a product of two cyclic groups of order $p-1$, and an element has odd order in $(\mathcal{O}/p\mathcal{O})^*$ if and only if it is a 2^kth power in $(\mathcal{O}/p\mathcal{O})^*$. As $q \in (\mathcal{O}/p\mathcal{O})^*$ is a 2^kth power if and only if p splits completely in the field $K(\zeta_{2^k}, \sqrt[2^k]{q})$, we conclude that a prime $p \in S_k^+$ does *not* divide a term of X_K if and only if it splits completely in $K(\zeta_{2^k}, \sqrt[2^k]{q})$, but not in $K(\zeta_{2^{k+1}}, \sqrt[2^k]{q})$. By the Chebotarev density theorem, the subset of such primes in S_k^+ has natural density $[K(\zeta_{2^k}, \sqrt[2^k]{q}) : \mathbb{Q}]^{-1} - [K(\zeta_{2^{k+1}}, \sqrt[2^k]{q}) : \mathbb{Q}]^{-1}$. The complement $D_k^+ = D^+ \cap S_k^+$ of this set in S_k^+ has a density as well, and we find that both $D^+ = \bigcup_{k \geq 1} D_k^+$ and its complement $S^+ \setminus D^+ = \bigcup_{k\geq 1}(S_k^+ \setminus D_k^+)$ in S^+ are countable disjoint unions of sets of primes having a natural density. It follows that D^+ has lower density $\sum_{k \geq 1} \delta(D_k^+)$, and that $S^+ \setminus D^+$ has lower density $\sum_{k\geq 1} \delta(S_k^+ \setminus D_k^+)$. These lower densities add up to $\delta(S^+)$, so they are in fact densities. We conclude that D^+ has a natural density δ_K^+ which satisfies

$$\frac{1}{2} - \delta_K^+ = \sum_{k \geq 1} \left(\frac{1}{[K(\zeta_{2^k}, \sqrt[2^k]{q}) : \mathbb{Q}]} - \frac{1}{[K(\zeta_{2^{k+1}}, \sqrt[2^k]{q}) : \mathbb{Q}]} \right). \tag{2.2}$$

Equation (2.2) reduces the computation of δ_K^+ to a computation of field degrees in the infinite extension $K(\zeta_{2^\infty}, \sqrt[2^\infty]{q})$ of $\mathbb{Q}$. To ease notation, we write

$$F_k = K(\zeta_{2^{k+1}}, \sqrt[2^k]{q}).$$

Then the kth term of the right hand side of (2.2) equals $[F_k : \mathbb{Q}]^{-1}$ if $\zeta_{2^{k+1}}$ generates a quadratic extension of $K(\zeta_{2^k}, \sqrt[2^k]{q})$, and 0 otherwise.

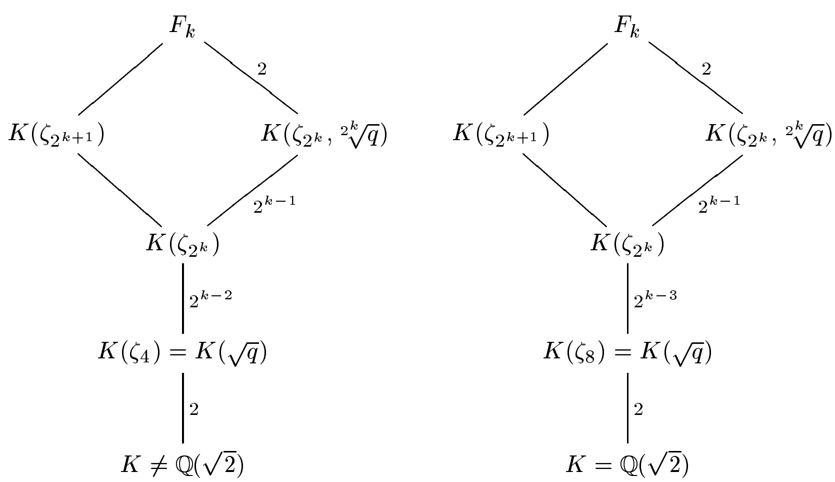
Suppose first that we have $N_{K/\mathbb{Q}}(\varepsilon) = -1$, and consequently $q = -\varepsilon^2$ in (2.1). Then q is a square in $K(\zeta_4)$, and also in the field $M = K(\zeta_{2^\infty})$ obtained by adjoining all 2-power roots of unity to K. It is not a fourth power in M, since M is abelian over $\mathbb{Q}$ and $M(\sqrt[4]{q}) = M(\sqrt{\varepsilon})$ has a quartic subfield $K(\sqrt{\varepsilon})$ that is not normal over $\mathbb{Q}$. By Kummer theory, it follows that $\sqrt[2^k]{q}$ generates a cyclic extension of degree 2^{k-1} of $K(\zeta_{2^k})$ for every $k \geq 2$. Our normality argument shows that this extension is linearly disjoint over $K(\zeta_{2^k})$ from $K(\zeta_{2^{k+1}})$.

For $k = 1$, we have a quadratic extension $K(\sqrt{q}) = K(\zeta_4)$, which coincides with the extension generated by $\zeta_{2^{k+1}} = \zeta_4$. This shows that in the case of norm -1, the term for $k = 1$ in (2.2) vanishes.

If K is not the real quadratic subfield $\mathbb{Q}(\sqrt{2})$ of $\mathbb{Q}(\zeta_{2^\infty})$, then $\zeta_{2^{k+1}}$ generates a quadratic extension of $K(\zeta_{2^k})$ for all $k \geq 2$, and F_k has degree $2 \cdot 2^k \cdot 2^{k-1} = 4^k$ for these k. We find $1/2 - \delta_K^+ = \sum_{k\geq 2} 4^{-k} = 1/12$ and $\delta_K^+ = 5/12$.

For $K = \mathbb{Q}(\sqrt{2})$ the degree of F_k is only $2^k \cdot 2^{k-1} = 2^{2k-1}$ for $k \geq 3$. Moreover, the term for $k = 2$ in (2.2) vanishes since $K(\zeta_4) = \mathbb{Q}(\zeta_8)$ now contains $\zeta_{2^{k+1}} = \zeta_8$. We find $1/2 - \delta_K^+ = \sum_{k\geq 3} 2^{1-2k} = 1/24$ and $\delta_K^+ = 11/24$.

The diagrams below indicate the field degrees in the two situations for $k \geq 2$ and $k \geq 3$, respectively.



Suppose next that we have $N_{K/\mathbb{Q}}(\varepsilon) = 1$, and so in particular $K \neq \mathbb{Q}(\sqrt{2})$. The analysis is similar to the previous case, but we now have $q = \varepsilon^2$, so q is a square in K. As the field $K(\sqrt[4]{\varepsilon})$ is non-normal of degree 8, we see that $q = \varepsilon^2$ is a square in $M = K(\zeta_{2^\infty})$, but not an eighth power. We have two cases.

Suppose q is *not* a fourth power in M. Then $\sqrt[2^k]{q}$ generates a cyclic extension of degree 2^{k-1} of $K(\zeta_{2^k})$ for every $k \geq 1$, and this extension is linearly disjoint from the extension of $K(\zeta_{2^k})$ generated by $\zeta_{2^{k+1}}$. This is similar to the case $K \neq \mathbb{Q}(\sqrt{2})$ above, the only difference being that we now also have a non-zero term for $k = 1$ in (2.2). We find $1/2 - \delta_K^+ = \sum_{k\geq 1} 4^{-k} = 1/3$ and $\delta_K^+ = 1/6$.

Suppose that q is a fourth power in M. Then $K(\sqrt{\varepsilon})$ is a subfield of M. Besides K, the quadratic subfields of $K(\sqrt{\varepsilon})$ are the two fields $\mathbb{Q}(\sqrt{\varepsilon}\pm 1/\sqrt{\varepsilon})$, and one of those two is contained in $\mathbb{Q}(\zeta_{2^\infty})$. From $N_{K/\mathbb{Q}}(\varepsilon) = 1$ we deduce

$$(2.3) \qquad (\sqrt{\varepsilon} \pm 1/\sqrt{\varepsilon})^2 = \mathrm{Tr}_{K/\mathbb{Q}}(\varepsilon) \pm 2 = 2(a \pm 1),$$

so this "exceptional case" occurs exactly when one of the elements $a \pm 1$ is a rational square. The fields $K(\zeta_4, \sqrt[4]{q}) = K(\zeta_4, \sqrt{\varepsilon})$ and $K(\zeta_8)$ coincide here, and $\sqrt[2^k]{q}$ generates, for all $k \geq 3$, a cyclic extension of degree 2^{k-2} of $K(\zeta_{2^k})$ that is linearly disjoint over $K(\zeta_{2^k})$ from $K(\zeta_{2^{k+1}})$. As in the case $K = \mathbb{Q}(\sqrt{2})$ above, the degree of F_k is only $2^k \cdot 2^{k-1} = 2^{2k-1}$ for $k \geq 3$. The term for $k = 2$ vanishes, but for $k = 1$ we do have a contribution $1/4$. We find $1/2 - \delta_K^+ = 1/4 + \sum_{k\geq 3} 2^{1-2k} = 7/24$ and $\delta_K^+ = 5/24$ if either $a+1$ or $a-1$ is a square. This shows that the values of δ_K^+ are as asserted.

Inert case. Let p be a prime that is inert in $K/\mathbb{Q}$. Then $\mathcal{O}/p\mathcal{O}$ is a field of p^2 elements, and the norm map $N : \mathcal{O}/p\mathcal{O} \to \mathbb{F}_p$ raises all elements to the power $p + 1$.

Suppose first that we are in the case $N_{K/\mathbb{Q}}(\varepsilon) = -1$. Then we have $q = -\varepsilon^2$ in (2.1) and $\varepsilon^{p+1} = -1 \in (\mathcal{O}/p\mathcal{O})^*$. For $p \equiv 1 \bmod 4$ we obtain $q^{(p+1)/2} = -\varepsilon^{p+1} = 1 \in (\mathcal{O}/p\mathcal{O})^*$, which shows that the order of q in $(\mathcal{O}/p\mathcal{O})^*$ is odd. For $p \equiv 3 \bmod 4$ we obtain $q^{(p+1)/2} = \varepsilon^{p+1} = -1 \in (\mathcal{O}/p\mathcal{O})^*$, which shows that the order of q in $(\mathcal{O}/p\mathcal{O})^*$ is even. We find that δ_K^- is the density of the primes $p \equiv 3 \bmod 4$ that are inert in $K/\mathbb{Q}$, hence $\delta_K^- = 1/4$.

From now on we suppose $N_{K/\mathbb{Q}}(\varepsilon) = 1$. In particular, this implies $K \neq \mathbb{Q}(\sqrt{2})$. We have $q = \varepsilon^2$, and consequently $q^{(p+1)/2} = \varepsilon^{p+1} = 1 \in (\mathcal{O}/p\mathcal{O})^*$ for all inert odd primes p. This shows that for all inert primes $p \equiv 1 \bmod 4$, the order of q is again odd and p does not divide a term of X_K. For the inert primes $p \equiv 3 \bmod 4$ we use an approach that is similar to that in the split case.

Let S^- be the set of odd primes p that are inert in $K/\mathbb{Q}$, and $D^- \subset S^-$ the set of primes in S^- that divide some term of X_K. For $k \in \mathbb{Z}_{\geq 2}$, we let $S_k^- \subset S^-$ be the set of primes $p \in S^-$ for which $p + 1$ has exactly $k = \mathrm{ord}_2(p + 1)$ factors 2. This is a set with a natural density, and we want to compute the density of the subset $D_k^- = D^- \cap S_k^-$ by characterizing the primes $p \in D_k^-$ in terms of splitting conditions on p in some finite Galois extension $F_k/\mathbb{Q}$.

A prime p is in S_k^- if and only if its Frobenius substitution in the abelian group $\mathrm{Gal}(K(\zeta_{2^{k+1}})/\mathbb{Q})$ is the unique element φ that is non-trivial on K and acts on the 2^{k+1}th roots of unity as $\varphi(\zeta_{2^{k+1}}) = \zeta_{2^{k+1}}^{-1+2^k}$. As $K(\zeta_{2^{k+1}})$ has degree 2^{k+1} over $\mathbb{Q}$, this shows that S_k^- has natural density 2^{-k-1} for all k. We let $B_k \subset K(\zeta_{2^{k+1}})$ be the subfield corresponding to the subgroup $\langle\varphi\rangle$ of $\mathrm{Gal}(K(\zeta_{2^{k+1}})/\mathbb{Q})$. Note that $K(\zeta_{2^{k+1}}) = B_k(\varepsilon)$ is a quadratic extension of B_k.

If p is in S_k^-, the order $p^2-1=(p-1)(p+1)$ of the cyclic group $(\mathcal{O}/p\mathcal{O})^*$ has exactly $k+1 \geq 3$ factors 2, and $q = \varepsilon^2 \in (\mathcal{O}/p\mathcal{O})^*$ has odd order if and only if ε^2 is a 2^{k+1}th power in $(\mathcal{O}/p\mathcal{O})^*$. As -1 is a 2^kth power in $(\mathcal{O}/p\mathcal{O})^*$, we conclude that $p \in S_k^-$ does not divide any term of X_K if and only if ε is a 2^kth power in $(\mathcal{O}/p\mathcal{O})^*$. This leads to a characterization of the primes $p \in S_k^-$ outside D^- in terms of their splitting behavior in the field

$$F_k = K(\zeta_{2^{k+1}}, \sqrt[2^k]{\varepsilon}) = B_k(\sqrt[2^k]{\varepsilon});$$

they are the primes p that split completely in B_k and have extensions in B_k that are inert in $B_k(\varepsilon)/B_k$ and split completely in $F_k/B_k(\varepsilon)$. This means that the Frobenius symbol of p in the non-abelian group $\mathrm{Gal}(F_k/\mathbb{Q})$, which is only determined up to conjugacy, is an element of order 2 in the normal subgroup $\mathrm{Gal}(F_k/B_k)$ that does not lie in the normal subgroup $\mathrm{Gal}(F_k/B_k(\varepsilon))$. If n_k denotes the number of such elements in $\mathrm{Gal}(F_k/\mathbb{Q})$, the Chebotarev density theorem yields an inert analogue of (2.2):

$$\frac{1}{2} - \delta_K^- = \frac{1}{4} + \sum_{k\geq 2} \frac{n_k}{[F_k:\mathbb{Q}]} = \frac{1}{4} + \sum_{k\geq 2} 2^{-k}\frac{n_k}{[F_k:B_k]}. \tag{2.4}$$

This time we have to do more than a degree computation, since we also need to know the structure of the group $\mathrm{Gal}(F_k/B_k)$.

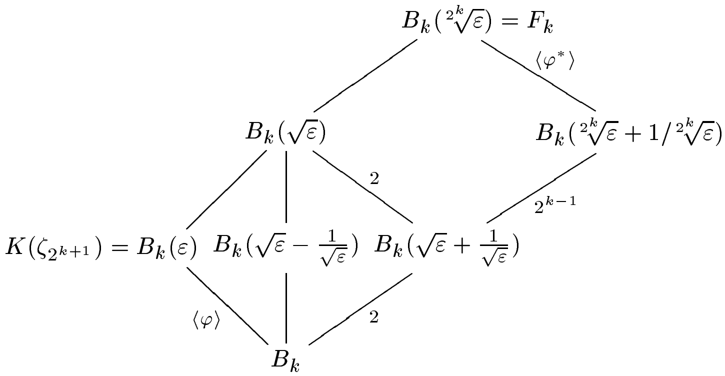
Suppose first that neither $a-1$ nor $a+1$ is a square. Then the extensions $K(\sqrt{\varepsilon})$ and $K(\zeta_{2^\infty})$ are linearly disjoint over K, and F_k is a cyclic extension of degree 2^k of $B_k(\varepsilon) = K(\zeta_{2^{k+1}})$ generated by $\sqrt[2^k]{\varepsilon}$. We can extend the generator φ of $\mathrm{Gal}(B_k(\varepsilon)/B_k)$ to an element $\varphi^* \in \mathrm{Gal}(F_k/B_k)$ of order 2 by setting $\varphi^*(\sqrt[2^k]{\varepsilon}) = 1/\sqrt[2^k]{\varepsilon}$. As φ^* acts by inversion on both $\langle\varepsilon\rangle$ and $\langle\zeta_{2^k}\rangle$, the Galois equivariance of the Kummer pairing

$$\mathrm{Gal}(F_k/B_k(\zeta_{2^{k+1}})) \times \langle\varepsilon\rangle \to \langle\zeta_{2^k}\rangle$$

shows that φ^* commutes with all elements in $\mathrm{Gal}(F_k/B_k(\varepsilon))$. We find

$$\mathrm{Gal}(F_k/B_k) \cong \mathrm{Gal}(F_k/B_k(\varepsilon)) \times \langle\varphi^*\rangle \cong \mathbb{Z}/2^k\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

As there are exactly two elements of order 2 in $\mathrm{Gal}(F_k/B_k)$ of the form (σ, φ^*), this yields $n_k = 2$ in (2.4) for all $k \geq 2$. We find $1/2 - \delta_K^- = 1/4 + \sum_{k\geq 2} 2^{-k}\cdot 2\cdot 2^{-k-1} = 1/3$ and $\delta_K^- = 1/6$.



Suppose finally that we are in the exceptional case where either $a+1$ or $a-1$ is a square. Then the extension F_k/B_k in the diagram above collapses to an extension of degree 2^k for all $k \geq 2$. For $k \geq 3$, we have $\sqrt{2} \in B_k$ and (2.3) shows that B_k contains $\sqrt{\varepsilon} + 1/\sqrt{\varepsilon}$ if $a+1$ is a square and $\sqrt{\varepsilon} - 1/\sqrt{\varepsilon}$ if $a-1$ is a square. In the first case we have an isomorphism

$$\mathrm{Gal}(F_k/B_k) \cong \mathrm{Gal}(B_k(\sqrt{\varepsilon})/B_k) \times \langle\varphi^*\rangle \cong \mathbb{Z}/2^{k-1}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

and $n_k = 2$ as before. In the other case, F_k/B_k is a cyclic extension of degree 2^k with quadratic subextension $B_k(\varepsilon) = B_k(\sqrt{\varepsilon})$. Any extension of $\varphi \in \mathrm{Gal}(B_k(\varepsilon)/B_k)$ to F_k is then a generator of $\mathrm{Gal}(F_k/B_k)$, and we have $n_k = 0$.

For $k = 2$, any of the elements $\sqrt{2}$ and $\sqrt{\varepsilon} \pm 1/\sqrt{\varepsilon}$ generates the quadratic extension $B_2(\sqrt{\varepsilon}) = B_2(\sqrt{2})$ of B_2. The extension $B_2 \subset B_2(\sqrt[4]{\varepsilon}) = F_2$ is of degree 4 and has a quadratic subextension generated by $\sqrt{\varepsilon} = \sqrt{(a+1)/2} + \sqrt{(a-1)/2}$. If $a+1$ is a square, then $\sqrt{\varepsilon}$ has norm -1 in B_k and F_2/B_2 is a cyclic extension. If $a-1$ is a square, then $\sqrt{\varepsilon}$ has norm 1 in B_k and F_2/B_2 is a V_4-extension. The corresponding values of n_2 are $n_2 = 0$ and $n_2 = 2$.

For $a+1$ a square we find $1/2 - \delta_K^- = 1/4 + 0 + \sum_{k\geq 3} 2^{-k} \cdot 2 \cdot 2^{-k} = 7/24$ and $\delta_K^- = 5/24$. For $a-1$ a square we find a finite sum $1/2 - \delta_K^- = 1/4 + 1/8$ and $\delta_K^- = 1/8$. This finishes the proof of the theorem.

References

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

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

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

[4] P. Moree, *On the prime density of Lucas sequences*, J. Théor. Nombres Bordeaux 8 (1996), 449–459.

[5] P. Ribenboim, *The New Book of Prime Number Records*, Springer, New York, 1995.
[6] P. Stevenhagen, *Prime densities for second order torsion sequences*, preprint.

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

Faculteit WINS
Universiteit van Amsterdam
Plantage Muidergracht 24
1018 TV Amsterdam, The Netherlands
E-mail: psh@wins.uva.nl

Received on 7.4.1997
and in revised form on 24.7.1997 (3165)