PRIME DIVISORS OF LUCAS SEQUENCES

Pieter Moree and Peter Stevenhagen

Abstract. The *Lucas sequence* associated to a real quadratic number field K is the integer sequence $X_K = \{\varepsilon^n + \bar\varepsilon^n\}_{n=0}^\infty$, with ε a fundamental unit in the ring of integers of K for which the trace $\varepsilon + \bar\varepsilon$ is positive. In this note, we determine for all real quadratic fields K the natural density of the set of prime numbers p that divide some term of the sequence X_K.

1. Introduction

Let $d > 1$ be a squarefree integer and $K = \mathbf{Q}(\sqrt{d})$ the corresponding real quadratic field. We write $\varepsilon = a + b\sqrt{d}$ for a fundamental unit in the ring of integers of K and define the *Lucas sequence* associated to K to be the integer sequence

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

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

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

for $n \geq 2$. If we take for K the field $\mathbf{Q}(\sqrt{5})$ generated by the golden ratio, we obtain the very classical example of the Lucas sequence with the familiar 'Fibonacci recursion' $x_n = x_{n-1} + x_n$ and 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 $N_{K/\mathbf{Q}}(\varepsilon)$ equals -1, when it is trivially determined. Clearly, one has $\delta_K = \delta_K^+ + \delta_K^-$.

The method in this note extends to sequences $\{\mathrm{Tr}_{K/\mathbf{Q}}(\alpha^n)\}_{n=0}^\infty = \{\alpha^n + \bar\alpha^n\}_{n=0}^\infty$, 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 in terms of α, this yields of 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 [4].

1991 *Mathematics Subject Classification.* Primary 11R45; Secondary 11B39.

Key words and phrases. Lucas sequence, Chebotarev density theorem.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

version April 20, 1997

Theorem. *Let $K = \mathbf{Q}(\sqrt{d})$ and $a = \frac{1}{2}\mathrm{Tr}_{K/\mathbf{Q}}(\varepsilon) > 0$ be as above. Then the natural densities δ_K^+ and δ_K^- for the sets of prime divisors of the Lucas sequence associated to K exist. For $N_{K/\mathbf{Q}}(\varepsilon) = -1$ 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 $N_{K/\mathbf{Q}}(\varepsilon) = 1$ the densities depend in the following way on whether the integers $a+1$ and $a-1$ are 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 [1]. Lagarias [2] was the first to use this idea in a quadratic setting, for the classical Lucas sequence mentioned above, which falls in the category $N_{K/\mathbf{Q}}(\varepsilon) = -1$. A generalization to other instances of units of norm -1 is given in [3].

2. Proof of the theorem.

Let $K = \mathbf{Q}(\sqrt{d})$ 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 $K/\mathbf{Q}$, then the kernel of the norm map $\kappa_p = \ker[N : (\mathcal{O}/p\mathcal{O})^* \to \mathbf{F}_p^*]$ is a cyclic group of order $p - \left(\frac{d}{p}\right)$. We set

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

Let $p \nmid 2d$ be a prime number. Looking at the explicit form of the n-th term $x_n = \varepsilon^n + \bar{\varepsilon}^n$ 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

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

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 $\mathbf{Q}$. We start with the easier case of the rational primes that split in K.

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

For $k \in \mathbf{Z}_{\geq 1}$, 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^k-th 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 $\delta(S_k^+) = [K(\zeta_{2^k}) : \mathbf{Q}]^{-1} - [K(\zeta_{2^{k+1}}) : \mathbf{Q}]^{-1}$. Clearly, the sum of these densities for all $k \geq 1$ is $[K : \mathbf{Q}]^{-1} = 1/2 = \delta(S^+)$.

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^k-th power in $(\mathcal{O}/p\mathcal{O})^*$. As $q \in (\mathcal{O}/p\mathcal{O})^*$ is a 2^k-th 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 $[K(\zeta_{2^k}, \sqrt[2^k]{q}) : \mathbf{Q}]^{-1} - [K(\zeta_{2^{k+1}}, \sqrt[2^k]{q}) : \mathbf{Q}]^{-1}$. 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

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

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 $\mathbf{Q}$. To ease notation we write

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

Then the k-th term of the right hand side of (2.2) equals $[F_k : \mathbf{Q}]^{-1}$ 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 $N_{K/\mathbf{Q}}(\varepsilon) = -1$, 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 as M is abelian over $\mathbf{Q}$ and $M(\sqrt[4]{q}) = M(\sqrt{\varepsilon})$ has a quartic subfield $K(\sqrt{\varepsilon})$ that is not normal over $\mathbf{Q}$. 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 the term for $k = 1$ always vanishes in (2.2).

If K is not the real quadratic subfield $\mathbf{Q}(\sqrt{2})$ of $\mathbf{Q}(\zeta_{2^\infty})$, 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 $\frac{1}{2} - \delta_K^+ = \sum_{k \geq 2} 4^{-k} = \frac{1}{12}$ and $\delta_K^+ = \frac{5}{12}$.

For $K = \mathbf{Q}(\sqrt{2})$ 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 $K(\zeta_4) = \mathbf{Q}(\zeta_8)$ now contains $\zeta_{2^{k+1}} = \zeta_8$. We find $\frac{1}{2} - \delta_K^+ = \sum_{k \geq 3} 2^{1-2k} = \frac{1}{24}$ and $\delta_K^+ = \frac{11}{24}$.

The diagrams below indicate the field degrees in the two situations for $k \geq 2$

and $k \geq 3$, respectively,

$$\begin{tikzcd}[arrows=dash]
& F_k \arrow[dl] \arrow[dr, "2"] & \\
K(\zeta_{2^{k+1}}) \arrow[dr] & & K(\zeta_{2^k}, \sqrt[2^k]{q}) \arrow[dl, "2^{k-1}"] \\
& K(\zeta_{2^k}) \arrow[d, "2^{k-2}"] & \\
& K(\zeta_4) = K(\sqrt{q}) \arrow[d, "2"] & \\
& K \neq \mathbf{Q}(\sqrt{2}) &
\end{tikzcd}
\qquad
\begin{tikzcd}[arrows=dash]
& F_k \arrow[dl] \arrow[dr, "2"] & \\
K(\zeta_{2^{k+1}}) \arrow[dr] & & K(\zeta_{2^k}, \sqrt[2^k]{q}) \arrow[dl, "2^{k-1}"] \\
& K(\zeta_{2^k}) \arrow[d, "2^{k-3}"] & \\
& K(\zeta_8) = K(\sqrt{q}) \arrow[d, "2"] & \\
& K = \mathbf{Q}(\sqrt{2}) &
\end{tikzcd}$$

Suppose next that we have $N_{K/\mathbf{Q}}(\varepsilon) = 1$, and so in particular $K \neq \mathbf{Q}(\sqrt{2})$. 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 $K \neq \mathbf{Q}(\sqrt{2})$ above, the only difference being that we now also have a non-zero term for $k = 1$ in (2.2). We find $\frac{1}{2} - \delta_K^+ = \sum_{k \geq 1} 4^{-k} = \frac{1}{3}$ and $\delta_K^+ = \frac{1}{6}$.

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 $\mathbf{Q}(\sqrt{\varepsilon} \pm 1/\sqrt{\varepsilon})$, and one of those two is contained in $\mathbf{Q}(\zeta_{2^\infty})$. ¿From $N_{K/\mathbf{Q}}(\varepsilon) = 1$ we deduce

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

so this happens exactly when one of the integers $a \pm 1$ is a square. The fields $K(\zeta_4, \sqrt[4]{q}) = K(\zeta_4, \sqrt{\varepsilon})$ and $K(\zeta_8)$ now coincide, 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 $K = \mathbf{Q}(\sqrt{2})$ above, the degree of F_k is now 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 $\frac{1}{4}$. We find $\frac{1}{2} - \delta_K^+ = \frac{1}{4} + \sum_{k \geq 3} 2^{1-2k} = \frac{7}{24}$ and $\delta_K^+ = \frac{5}{24}$ if $a + 1$ 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 $K/\mathbf{Q}$. Then $\mathcal{O}/p\mathcal{O}$ is a field of p^2 elements, and the norm map $N : \mathcal{O}/p\mathcal{O} \to \mathbf{F}_p$ raises all elements to the power $p+1$.

Suppose first that we are in the case $N_{K/\mathbf{Q}}(\varepsilon) = -1$. 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 $K/\mathbf{Q}$ and equals $\delta_K^- = 1/4$.

¿From now on we suppose $N_{K/\mathbf{Q}}(\varepsilon) = 1$. In particular, this implies $K \neq \mathbf{Q}(\sqrt{2})$. 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 $K/\mathbf{Q}$, and $D^- \subset S^-$ the set of primes in S^- that divide some term of X_K. For $k \in \mathbf{Z}_{\geq 2}$, 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 $F_k/\mathbf{Q}$.

A prime p is in S_k^- if and only if its Frobenius substitution in the abelian group $\mathrm{Gal}(K(\zeta_{2^{k+1}})/\mathbf{Q})$ 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 $\mathbf{Q}$, 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 $\mathrm{Gal}(K(\zeta_{2^{k+1}})/\mathbf{Q})$. 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^k-th 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^k-th 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 in $F_k/B_k(\varepsilon)$. This means that the Frobenius symbol of p in the non-abelian group $\mathrm{Gal}(F_k/\mathbf{Q})$, 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 $\mathrm{Gal}(F_k/\mathbf{Q})$, the Chebotarev density theorem yields an inert analogue of (2.2):

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

This time we have to do slightly 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 $F_k/B_k(\varepsilon)$ is a cyclic extension of degree 2^k 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-equivariancy of the Kummer pairing

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

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

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

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 $\frac{1}{2} - \delta_K^- = \frac{1}{4} + \sum_{k\geq 2} 2^{-k} \cdot 2 \cdot 2^{-k-1} = \frac{1}{3}$

and $\delta_K^- = \frac{1}{6}$.

$$\begin{tikzcd}[column sep=small]
 & & B_k(\sqrt[2^k]{\varepsilon}) = F_k \arrow[dl, dash] \arrow[dr, dash, "\langle\varphi^*\rangle"] & \\
 & B_k(\sqrt{\varepsilon}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash, "2"] & & B_k(\sqrt[2^k]{\varepsilon} + 1/\sqrt[2^k]{\varepsilon}) \arrow[dl, dash, "2^{k-1}"] \\
K(\zeta_{2^{k+1}}) = B_k(\varepsilon) \arrow[dr, dash, "\langle\varphi\rangle"'] & B_k(\sqrt{\varepsilon} - \frac{1}{\sqrt{\varepsilon}}) \arrow[d, dash] & B_k(\sqrt{\varepsilon} + \frac{1}{\sqrt{\varepsilon}}) \arrow[dl, dash, "2"] & \\
 & B_k & &
\end{tikzcd}$$

Suppose now that 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

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

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

References

1. H. Hasse, *Über die Dichte der Primzahlen p, für die eine vorgegebene rationale Zahl $a \neq 0$ von durch eine vorgegebene Primzahl $l \neq 2$ teilbarer bzw. unteilbarer Ordnung mod p ist*, Math. Ann. **162** (1965), 74–76.
2. 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.
3. P. Moree, *On the prime density of Lucas sequences*, J. Théor. Nombres Bordeaux **8** (1996), 449–459.
4. P. Moree and P. Stevenhagen, *Prime densities for linear recurrences* (in preparation).
5. P. Ribenboim, *The new book of prime number records*, Springer, New York, 1995.

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, Plantage Muidergracht 24, 1018 TV Amsterdam, The Netherlands

E-mail address: psh@wins.uva.nl