On the prime density of Lucas sequences

Pieter Moree

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

Germany

MPI 96-67

On the prime density of Lucas sequences

Pieter Moree

May 31, 1996

Abstract

For any integer P, let $\{L_n(P)\}_{n=0}^{\infty}$ be the Lucas sequence defined by $L_0(P) = 2$, $L_1(P) = P$ and, for every $n \geq 2$, $L_n(P) = PL_{n-1}(P) + L_{n-2}(P)$. The density of the set of primes dividing this sequence is computed.

1 Introduction

If S is any set of integers, then by $S(x)$ we denote the number of elements in S not exceeding x. The limit $\lim_{x\to\infty} S(x)/\pi(x)$, if it exists, is called the prime density of S. It will be denoted by $\delta(S)$.

Let $\mathbb{Q}(\sqrt{D})$ be a real quadratic field with $D > 1$ and D squarefree. (This assumption on D is maintained throughout.) Let $\mathfrak{O}_D$ denote its ring of integers. Suppose $\mathfrak{O}_D$ contains a unit of norm -1. Then obviously the fundamental unit, ϵ_D, has norm -1. Let $u \neq \pm 1$ be a unit of $\mathfrak{O}_D$. In this paper we are interested in computing the prime density of the sequence $u^n + \bar{u}^n$. The sequence $u^n + \bar{u}^n$ has an irreducible characteristic polynomial over $\mathbb{Q}$. Few people seem to have considered this problem. The papers [4, 5] are the only ones known to the author in this direction. In contrast several authors [1, 3, 6, 9] considered the prime density of second order linear recurrences having reducible characteristic polynomial (i.e. sequences of the form $a^n + b^n$).

Our main result is the following.

Theorem 1 *Let $\mathbb{Q}(\sqrt{D})$ be a real quadratic field with $D > 1$ and D squarefree having a unit of negative norm. Let $u \neq \pm 1$ be a unit. Then there exists $\lambda \geq 0$ and ϵ of norm -1 such that $u = \epsilon^{2^\lambda}$. The sequence $u^n + \bar{u}^n$ has a prime density. In case $D = 2$ it is given by $17/24$ if $\lambda = 0$, $5/12$ if $\lambda = 1$ and $2^{-\lambda}/3$ otherwise. In case $D > 2$ the prime density equals $2^{1-\lambda}/3$.*

It should be remarked that the question whether a quadratic field has a unit of negative norm is still not satisfactorily resolved. If D has a prime divisor $p \equiv 3 \pmod 4$, then there is no such unit. From this it easily follows that there are at most $O(x/\sqrt{\log x})$ discriminants $D \leq x$ for which there is a negative unit. Stevenhagen conjectures that there are asymptotically $cx/\sqrt{\log x}$ such discriminants, for some constant $c > 0$. For more on this topic see e.g. [8].

Theorem 1 allows one to compute the density of the Lucas sequence defined by

$V_0(P) = 2,\ V_1(P) = P$ and $V_n(P) = PV_{n-1}(P) - V_{n-2}(P)$ for various P. For example the sequence $\{V_n(326)\}$ has density $5/12$. More interestingly Theorem 1 allows one to calculate for every integer P the prime density of the Lucas sequence $L_n(P) = PL_{n-1}(P)+L_{n-2}(P)$. In this the sequence $\{L_n(2)\}_{n=0}^{\infty} = \{2, 2, 6, 14, 34, \cdots\}$, the so called Pell sequence, plays an important rôle.

Theorem 2 *For P any nonzero integer let $\{L_n(P)\}_{n=0}^{\infty}$ be the Lucas sequence defined by $L_0(P) = 2,\ L_1(P) = P$ and, for $n \geq 2$, $L_n(P) = PL_{n-1}(P) + L_{n-2}(P)$. Then the prime density of this sequence exists and equals $2/3$, unless $|P| = L_n(2)$ for some odd $n \geq 1$, in which case the density is $17/24$.*

On taking $P = 1$ we find that the prime density of the sequence of Lucas numbers equals $2/3$. This was first proved by Lagarias [4]. Taking $P = 2$ it is seen that the prime density of the Pell sequence is $17/24$.

2 Outline of the proofs

The arithmetic of the sequence $\{\alpha^n + \bar{\alpha}^n\}$, where $\alpha \in \mathbb{Q}(\sqrt{D})$, is intimately connected with that of the sequence $\{W_n\}$, where $W_n := (\alpha^n - \bar{\alpha}^n)/(\alpha - \bar{\alpha})$. This sequence can be alternatively defined by $W_0 = 0,\ W_1 = 1,\ W_n = Tr(\alpha)W_{n-1} + W_{n-2}$ for $n \geq 2$. It is a Lucas sequence (see [7, p. 41] for a definition). We recall some facts from [7, pp. 41-60]. For primes p with $(p, 2N(\alpha)) = 1$, there exists a smallest index $\rho_\alpha(p) \geq 1$ such that $p|W_{\rho_\alpha(p)}$. The index $\rho_\alpha(p)$ is called the rank of apparition of p in $\{W_n\}$. If $(p, 2N(\alpha)) = 1$, then $p|W_n$ if and only if $\rho_\alpha(p)|n$. Furthermore $W_{2n} = W_n A_n$ and $(W_n, A_n)|2$. Using the latter three properties it can be easily shown that if $(p, 2N(\alpha)) = 1$, then p divides $\{W_n\}$ if and only if $\rho_\alpha(p)$ is even (cf. [5, Lemma 1]). From the theory of Lucas sequences it is known that if p is odd and $p|D$, then $\rho_\alpha(p)$ is odd. If $p \nmid D$ and $p \equiv 3 (\text{mod } 4)$, then $\rho_\alpha(p)$ is even. If $p \nmid D$ and $p \equiv 1 (\text{mod } 4)$ and $(D/p) = -1$, then $\rho_\alpha(p)$ is odd. Thus, using Lemma 4, one deduces that the density of $\{W_n\}$ is in $[1/2, 3/4]$. Indeed our approach to compute the prime density of $\{W_n\}$ is to compute the density of primes for which $\rho_\alpha(p)$ is even. We will actually compute the prime density of $\{p : 2^e || \rho_\alpha(p)\}$ for every $e \geq 0$, as this requires only little additional effort. It will allow us to deal with the case $\lambda \geq 1$ in Theorem 1. The fact that, for $(p, N(\alpha)Tr(\alpha)D) = 1$, $\rho_\alpha(p)$ divides $p - (D/p)$, forces us to consider the cases $(D/p) = 1$ and $(D/p) = -1$ seperately. For $s = 1, 2,\ e \geq 0,\ j \geq 1$ put

$$N_s(e, j; \alpha) = \{p :\ (p, 2N(\alpha)) = 1,\ (\frac{D}{p}) = 3-2s,\ p \equiv 3-2s+2^j (\text{mod } 2^{j+1}),\ 2^e || \rho_\alpha(p)\}.$$

We show that $N_s(e, j; \alpha)$ has a prime density, $\delta_s(e, j; \alpha)$, and compute it. In the case $s = 1$ this is done by relating $\delta_1(e, j; \alpha)$ to degrees of certain Kummerian extensions. This approach goes back to Hasse [3]. In the case $s = 2$ more elementary arguments suffice. It is then not difficult to show that the prime density of the sequence $\{W_n\}$ with $N(\alpha) = -1$ is given by

$$1 - \sum_{j=1}^{\infty} \{\delta_1(0, j; \alpha) + \delta_2(0, j; \alpha)\}.$$

$N_1(e,j;\alpha)$ and $N_2(e,j;\alpha)$ are computed in respectively §3 and §4. They are tabulated in Tables I and II. The entry e in the last column gives $\sum_{j=1}^{\infty}\delta_s(e,j;\alpha)$. The entry j in the last row gives $\sum_{e=0}^{\infty}\delta_s(e,j;\alpha)$. The distinction between the case $D=2$ and $D>2$ is due to the fact that for $j\geq 3$ the only real quadratic subfield of $\mathbb{Q}(\zeta_{2^j})$ is $\mathbb{Q}(\sqrt{2})$. Finally in §5 the proofs of Theorem 1 and 2 are given.

3 The prime divisors of Lucas sequences splitting in the associated quadratic number field

In this section the prime density of the set $N_1(e,j;\alpha)$ will be computed by relating it to the degrees of certain finite extensions of $\mathbb{Q}$ (Lemma 1). In Lemma 3 these degrees are then computed in case $N(\alpha)=-1$. Using Lemma 1 and Lemma 3 one easily arrives at Table I.1 and II.1. The fact that the second column in Table I.1 only contains zero entries is due to the fact that there are no primes satisfying $(2/p)=1$ and $p\equiv 5(\text{mod } 8)$.

Lemma 1 *Let $\alpha\in\mathbb{Q}(\sqrt{D})\backslash\mathbb{Q}$ be a quadratic integer. Put $\theta=\alpha^2/N(\alpha)$. For $0\leq r\leq s$ put $K_{r,s}=\mathbb{Q}(\sqrt{D},\theta^{1/2^r},\zeta_{2^s})$. Let $d_{r,s}=[K_{r,s}:\mathbb{Q}]$. Let $j\geq 1$ and $0\leq e\leq j$. Then the prime density, $\delta_1(e,j;\alpha)$, of*

$$N_1(e,j;\alpha):=\{p:(p,2N(\alpha))=1,\left(\frac{D}{p}\right)=1,\ p\equiv 1+2^j(\text{mod } 2^{j+1}),\ 2^e\|\rho_\alpha(p)\}$$

exists. In case $e=0$,

$$\delta_1(0,j;\alpha)=\frac{1}{d_{j,j}}-\frac{1}{d_{j,j+1}}.$$

In case $e\geq 1$,

$$\delta_1(e,j;\alpha)=\frac{1}{d_{j-e,j}}-\frac{1}{d_{j-e,j+1}}-\frac{1}{d_{j-e+1,j}}+\frac{1}{d_{j-e+1,j+1}}.$$

Furthermore $\delta_1(e,j;\alpha)=0$ in case $e>j$.

Proof: Some details of the proof will be surpressed. The reader having difficulties supplying the missing details is referred to [5]. If $(D/p)=1$ then p splits in $\mathbb{Q}(\sqrt{D})$. So $(p)=\mathfrak{P}\bar{\mathfrak{P}}$ in $\mathfrak{O}_D$. If $(p,2N(\alpha))=1$, then $\text{ord}_{\mathfrak{P}}(\theta)=\ \text{ord}_{\bar{\mathfrak{P}}}(\theta)=\rho_\alpha(p)$. Using that for all large enough primes satisfying $(D/p)=1$, $\rho_\alpha(p)|p-1$, it follows that $N_1(e,j;\alpha)$ is finite in case $e>j$. Then $\delta_1(e,j;\alpha)=0$. Now assume $e\leq j$. Let $\sigma_\alpha(p)$ denote the exact power of 2 dividing $\rho_\alpha(p)$. Put

$$S_j=\{p:\left(\frac{D}{p}\right)=1,\ (p,2N(\alpha))=1,\ p\equiv 1+2^j(\text{mod } 2^{j+1})\}.$$

Then the set $N_1(e,j;\alpha)$ equals

$$\{p:p\in S_j,\ \sigma_\alpha(p)|2^e\}\backslash\{p:p\in S_j,\ \sigma_\alpha(p)|2^{e-1}\}.$$

This, on its turn, can be written as $\{p : p \in S_j,\ \theta^{\frac{p-1}{2^j}} \equiv 1(\bmod\ \mathfrak{P})\}$ if $e = 0$ and

$$\{p : p \in S_j,\ \theta^{\frac{p-1}{2^{j-e}}} \equiv 1(\bmod\ \mathfrak{P})\}\backslash\{p : p \in S_j,\ \theta^{\frac{p-1}{2^{j-e+1}}} \equiv 1(\bmod\ \mathfrak{P})\}$$

otherwise. The latter set equals

$$\{p : \left(\frac{D}{p}\right) = 1,\ (p, 2N(\alpha)) = 1,\ p \equiv 1(\bmod\ 2^j),\ \theta^{\frac{p-1}{2^{j-e+1}}} \equiv 1(\bmod\ \mathfrak{P})\}$$

with the subset

$$\{p : \left(\frac{D}{p}\right) = 1,\ (p, 2N(\alpha)) = 1,\ p \equiv 1(\bmod\ 2^{j+1}),\ \theta^{\frac{p-1}{2^{j-e+1}}} \equiv 1(\bmod\ \mathfrak{P})\}$$

taken out. The latter set equals, with at most finitely many exceptions, the set of primes that split completely in $K_{j-e+1,j+1}$. Since for $r \le s$, $K_{r,s}$ is normal over $\mathbb{Q}$, it follows by the prime ideal theorem or by the Chebotarev density theorem that the prime density of this set equals $d^{-1}_{j-e+1,j+1}$. The density of the other sets involved are computed similarly. One finds $\delta_1(0, j; \alpha) = d^{-1}_{j,j} - d^{-1}_{j,j+1}$ and, in the case $e \ge 1$, $\delta_1(e, j; \alpha) = d^{-1}_{j-e,j} - d^{-1}_{j-e,j+1} - d^{-1}_{j-e+1,j+1} + d^{-1}_{j-e+1,j+1}$. □

In our computation of the degrees $d_{a,b}$ we will make use of the following easy lemma.

Lemma 2 [2, Satz 1]
The field $\mathbb{Q}(\sqrt{\alpha})$ with $\alpha \in \mathbb{Q}(\sqrt{D})\backslash\mathbb{Q}$ is normal over $\mathbb{Q}$ if and only if $N(\alpha)$ is a square in $\mathbb{Q}(\sqrt{D})$.

Lemma 3 *Suppose that $\alpha > 0$, $\alpha \in \mathbb{Q}(\sqrt{D})$, is a unit of negative norm.*
(i) *$D = 2$. We have $d_{0,1} = 2$, $d_{0,2} = 4$ and $d_{0,b} = 2^{b-1}$ for $b \ge 3$. Furthermore $d_{1,1} = 4$, $d_{1,b} = d_{0,b}$ for $b \ge 2$. For $b > a \ge 2$, $d_{a,b} = 2^{a+b-2}$. Finally, $d_{2,2} = 8$ and $d_{j,j} = 2^{2j-2}$ for $j \ge 3$.*
(ii) *$D > 2$. We have for $b > a \ge 1$, $d_{a,b} = 2^{a+b-1}$. 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: (i). Since $\sqrt{2} \in \mathbb{Q}(\zeta_8)$, we have, for $b \ge 3$, $\mathbb{Q}(\sqrt{2}, \zeta_{2^b}) = \mathbb{Q}(\zeta_{2^b})$ and thus $d_{0,b} = 2^{b-1}$. For $a = 1$, $b \ge 2$ we have $\mathbb{Q}(\sqrt{2}, \sqrt{-\alpha^2}, \zeta_{2^b}) = \mathbb{Q}(\sqrt{2}, i, \zeta_{2^b}) = \mathbb{Q}(\sqrt{2}, \zeta_{2^b})$. Thus $d_{1,b} = d_{0,b}$ for $b \ge 2$. Now assume that $b > a \ge 2$. Then $\mathbb{Q}(\sqrt{2}, (-\alpha^2)^{1/2^a}, \zeta_{2^b}) = \mathbb{Q}(\sqrt{2}, \alpha^{1/2^{a-1}}, \zeta_{2^b}) = \mathbb{Q}(\alpha^{1/2^{a-1}}, \zeta_{2^b})$. I claim that $x^{2^{a-1}} - \alpha$ is irreducible over $\mathbb{Q}(\zeta_{2^b})$. If it were not, then $\mathbb{Q}(\sqrt{\alpha})$ would be a subfield of $\mathbb{Q}(\zeta_{2^b})$ and hence normal. But since $\mathbb{Q}(\sqrt{\alpha})$ is not normal by Lemma 2, this is impossible. Thus $[\mathbb{Q}(\alpha^{1/2^{a-1}}, \zeta_{2^b}) : \mathbb{Q}] = [\mathbb{Q}(\alpha^{1/2^{a-1}} : \mathbb{Q}(\zeta_{2^b})][\mathbb{Q}(\zeta_{2^b}) : \mathbb{Q}] = 2^{a+b-2}$. Next consider the field $\mathbb{Q}(\sqrt{2}, (-\alpha^2)^{1/2^b}, \zeta_{2^b})$ for $b \ge 3$. Note that

$$\mathbb{Q}(\sqrt{2}, (-\alpha^2)^{1/2^b}, \zeta_{2^b}) = \mathbb{Q}(\sqrt{2}, \alpha^{1/2^{b-2}}, \zeta_{2^b}, \sqrt{\alpha^{1/2^{b-2}}\zeta_{2^b}}).$$

By taking composita with $\mathbb{Q}(\zeta_{2^{b+1}})$ one sees that

$$r := [\mathbb{Q}(\sqrt{2}, \alpha^{1/2^{b-2}}, \zeta_{2^b}, \sqrt{\alpha^{1/2^{b-2}}\zeta_{2^b}}) : \mathbb{Q}(\sqrt{2}, \alpha^{1/2^{b-2}}, \zeta_{2^b})] = 2.$$

Thus $d_{b,b} = rd_{b-1,b} = 2^{2b-2}$. Finally one checks that the missing degrees, $d_{0,1}$, $d_{0,2}$, $d_{1,1}$ and $d_{2,2}$, are as asserted.
(ii). We only deal with the case $b > a \geq 2$. The other cases are even more similar to (i) and left to the reader (see also [5, Lemma 6]). We have $\mathbb{Q}(\sqrt{D}, (-\alpha^2)^{1/2^a}, \zeta_{2^b}) = \mathbb{Q}(\sqrt{D}, \alpha^{1/2^{a-1}}, \zeta_{2^b})$. I claim that $X^{2^{a-1}} - \alpha$ is irreducible over $\mathbb{Q}(\sqrt{D}, \zeta_{2^b})$. Note that the latter field, as a compositum of two abelian fields, is itself abelian. Hence all its subfields are normal. Now if $X^{2^{a-1}} - \alpha$ were reducible over $\mathbb{Q}(\sqrt{D}, \zeta_{2^b})$, $\mathbb{Q}(\sqrt{\alpha})$ would be a subfield of $\mathbb{Q}(\sqrt{D}, \zeta_{2^b})$. By Lemma 2 this is seen to be impossible. The degree $d_{a,b}$ is then computed as in (i). □

4 The prime divisors of Lucas sequences inert in the associated quadratic number field

As will be seen, in case α is a unit of negative norm, the problem of computing the density $\delta_2(e, j; \alpha)$ can be easily reduced to that of computing the density of $\{p : (D/p) = -1,\ p \equiv -1 + 2^j (\text{mod } 2^{j+1})\}$. For $D > 2$ this density is computed in the next lemma.

Lemma 4 *Let $D > 2$ be squarefree. Put*

$$R_j = \{p : \left(\frac{D}{p}\right) = 1,\ p \equiv -1 + 2^j (\text{mod } 2^{j+1})\}.$$

Then $\delta(R_j)$, the prime density of R_j, equals 2^{-1-j}.

Proof: Consider the set of primes

$$S_j := \{p : \left(\frac{D}{p}\right) = 1,\ p \equiv -1 (\text{mod } 2^j)\}.$$

Now $(D/p) = 1$ and $p \equiv \pm 1 (\text{mod } 2^j)$ if and only if the prime p splits completely in $\mathbb{Q}(\sqrt{D}, \zeta_{2^j} + \zeta_{2^j}^{-1})$. Similarly $(D/p) = 1$ and $p \equiv 1 (\text{mod } 2^j)$ if and only if p splits completely in $\mathbb{Q}(\sqrt{D}, \zeta_{2^j} + \zeta_{2^j}^{-1})$ but does not split completely in $\mathbb{Q}(\sqrt{D}, \zeta_{2^j})$. Since both of these number fields are normal extensions of $\mathbb{Q}$, it follows by the Chebotarev density theorem that

$$\delta(S_j) = \frac{1}{[\mathbb{Q}(\sqrt{D}, \zeta_{2^j} + \zeta_{2^j}^{-1}) : \mathbb{Q}]} - \frac{1}{[\mathbb{Q}(\sqrt{D}, \zeta_{2^j}) : \mathbb{Q}]}.$$

Since $[\mathbb{Q}(\sqrt{D}, \zeta_{2^j}) : \mathbb{Q}(\sqrt{D}, \zeta_{2^j} + \zeta_{2^j}^{-1})] | 2$ and $\mathbb{Q}(\sqrt{D}, \zeta_{2^j})$ as a totally real field is strictly included in $\mathbb{Q}(\sqrt{D}, \zeta_{2^j})$, it follows that $\delta(S_j) = [\mathbb{Q}(\sqrt{D}, \zeta_{2^j}) : \mathbb{Q}]^{-1}$. Since the only real quadratic subfield of $\mathbb{Q}(\zeta_{2^j})$ is at most $\mathbb{Q}(\sqrt{2})$, it follows that $[\mathbb{Q}(\sqrt{D}, \zeta_{2^j}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{D}) : \mathbb{Q}][\mathbb{Q}(\zeta_{2^j}) : \mathbb{Q}] = 2^j$ and hence $\delta(S_j) = 2^{-j}$. Now notice that $R_j = S_j \backslash S_{j+1}$. Thus $\delta(R_j) = \delta(S_j) - \delta(S_{j+1}) = 2^{-1-j}$. □

Remark. From the law of quadratic reciprocity one deduces that for odd D, $(D/p) = 1$ if and only if $p \equiv \pm\beta (\text{mod } 4D)$ for a set of odd β (this result was already conjectured by Euler). This set has $\varphi(D)/2$ elements. Using this, the supplementary law of quadratic reciprocity, the chinese remainder theorem and the prime number theorem for arithmetic progressions, one can give an alternative proof of Lemma 4.

Let ϵ be a unit of negative norm. Now we are in the position to compute $\delta_2(e, j; \epsilon)$. For primes inert in $\mathbb{Q}(\sqrt{D})$, $\mathbb{Z}[\epsilon]/(p) \cong \mathbb{F}_{p^2}$, and hence the Frobenius map acts by conjugation on ϵ, that is $\epsilon^p \equiv \bar{\epsilon} (\text{mod } (p))$. Thus, since $N(\epsilon) = -1$, we have $\epsilon^{p+1} \equiv -1 (\text{mod } (p))$. Hence if $p \equiv -1 + 2^j (\text{mod } 2^{j+1})$, $j \geq 2$, then $\theta^{\frac{p+1}{2}} = (-1)^{\frac{p+1}{2}} \epsilon^{p+1} \equiv -1 (\text{mod } (p))$. Thus $2^j \| \text{ord}_{(p)}(\theta)$ $(= \rho_\epsilon(p))$ and therefore $N_2(j, j; \epsilon) = \{p : (D/p) = -1,\ p \equiv -1 + 2^j (\text{mod } 2^{j+1})\}$. In the case $D > 2$, $j \geq 2$, $\Delta_2(j, j; \epsilon) = 2^{-j-1}$, by Lemma 4. If $D = 2$, then $\Delta_2(j, j; \epsilon) = 0$ for $j \geq 3$ and $N_2(2, 2; \epsilon) = \{p :\ p \equiv 3 (\text{mod } 8)\}$, that is $\Delta_2(2, 2; \epsilon) = 1/4$. In case $j = 1$, $p \equiv 1 (\text{mod } 4)$ and so $\theta^{\frac{p+1}{2}} = (-1)^{\frac{p+1}{2}} \epsilon^{p+1} \equiv 1 (\text{mod } (p))$. Since $(p+1)/2$ is odd, $N_2(0, 1; \epsilon) = \{p : (D/p) = -1,\ p \equiv 1 (\text{mod } 4)\}$. If $D > 2$, then $\Delta_2(0, 1; \epsilon) = 1/4$ by Lemma 4. If $D = 2$ then $N_2(0, 1; \epsilon) = \{p : p \equiv 5 (\text{mod } 8)\}$ and so $\Delta_2(0, 1; \epsilon) = 1/4$. Thus we arrive at Table I.2 and Table II.2.

5 Proofs of Theorems 1 and 2

Theorem 1 is easily deduced from the following theorem.

Theorem 3 *Let ϵ be a unit of negative norm in $\mathcal{O}_D$. Let $\rho_\epsilon(p)$ denote the rank of apparition of p in the sequence $\{\epsilon^n + \bar{\epsilon}^n\}$. Consider for $e \geq 0$ the prime density of the set $\{p : 2^e \| \rho_\epsilon(p)\}$. In case $D = 2$ it equals $7/24$ if $e \leq 1$, $1/3$ if $e = 2$ and $2^{-e}/3$ for $e \geq 3$. In case $D > 2$ it equals $1/3$ if $e = 0$ and $2^{1-e}/3$ if $e \geq 1$.*

Proof: Let $N(e, \epsilon) = \{p : 2^e \| \rho_\epsilon(p)\}$ and for $s = 1, 2$ let

$$N_s(e; \epsilon) = \{p : (D/p) = 3 - 2s,\ 2^e \| \rho_\epsilon(p)\}.$$

Thus, with at most finitely many exceptions, $N(e; \epsilon) = N_2(e; \epsilon) \cup N_2(e; \epsilon)$. Now $N_1(e; \epsilon) = \cup_{j=1}^\infty N_1(e, j; \epsilon)$ and $N_2(e; \epsilon) = \cup_{j=1}^\infty N_2(e, j; \epsilon)$. Since the latter is a finite disjoint union of sets of non-zero density, we have $\delta_2(e; \epsilon) = \sum_{j=1}^\infty \delta_2(e, j; \epsilon)$. Similarly we want to show that $\delta_1(e; \epsilon) = \sum_{j=1}^\infty \delta_1(e, j; \epsilon)$. As $\cup_{j=1}^\infty N_1(e, j; \epsilon)$ is an infinite union of sets of non-zero density, this needs proof. We proceed as in [4, p. 454]. Put

$$C_1(e, j; \epsilon) = \{p : (D/p) = 1,\ p \equiv 1 + 2^j (\text{mod } 2^{j+1}) \text{ and } p \notin N_1(e, j, \epsilon)\}.$$

Using Lemma 4 the density of this set is seen to be $2^{-j} - \delta_1(e, j; \epsilon)$ in case $D = 2$ and $j \geq 3$, and $2^{-1-j} - \delta_1(e, j; \epsilon)$ in case $D > 2$. Now

$$\cup_{j=1}^m N_1(e, j; \epsilon) \subseteq N_1(e; \epsilon) \subseteq \{p : (D/p) = 1\} \setminus \cup_{j=1}^m C_1(e, j; \epsilon).$$

The smallest set in the above inclusion of sets has density $\sum_{j=1}^m \delta_1(e, j; \epsilon)$. The largest set has prime density $2^{-m} + \sum_{j=1}^m \delta_1(e, j; \epsilon)$ in case $D = 2$ and $m \geq 3$ and prime density $2^{-1-m} + \sum_{j=1}^m \delta_1(e, j; \epsilon)$ in case $D > 2$. Letting $m \to \infty$ shows that $\delta_1(e; \epsilon) = \sum_{j=1}^\infty \delta_1(e, j; \epsilon)$. On computing the densities $\sum_{j=1}^\infty \{\delta_1(e, j; \epsilon) + \delta_2(e, j; \epsilon)\}$, on making use of Lemma 1 and Lemma 3, the proof is then completed. □

Proof of Theorem 1. Since the prime density of $\{u^n+\bar{u}^n\}$ is invariant under replacing u by $\bar{u}$, $-u$ or $-\bar{u}$ and, by assumption, $u \neq \pm 1$, we may assume w.l.o.g. that $u > 1$. Then $u = \epsilon_D^N$ for some $N > 1$. Write $N = 2^\lambda m$ with m odd. Put $\epsilon = \epsilon_D^m$. Then $u = \epsilon^{2^\lambda}$ with $N(\epsilon) = -1$. Note that λ is unique. Consider the sequence $\{u^n + \bar{u}^n\}$ as a subsequence of $\{\epsilon^n + \bar{\epsilon}^n\}$. One easily shows that p divides $\{\epsilon^{2^\lambda n} + \bar{\epsilon}^{2^\lambda n}\}$ if and only if $\rho_\epsilon(p)$ is divisible by $2^{\lambda+1}$. Hence the prime density of $\{u^n + \bar{u}^n\}$ equals

$$1 - \sum_{m=0}^{\lambda} \delta(\{p : 2^m || \rho_\epsilon(p)\}).$$

Using this expression and Theorem 3, Theorem 1 now follows. □

Proof of Theorem 2. Put $D = P^2 + 4$. Notice that for $P \neq 0$, D is not a square. We have $L_n(P) = \alpha^n + \bar{\alpha}^n$ with $\alpha = (P + \sqrt{D})/2$. If $D \equiv 0 \pmod 4$ then $\alpha \in \mathbb{Z}[\sqrt{D}]$, if $D \equiv 1 \pmod 4$ then $\alpha \in \mathbb{Z}[(1+\sqrt{D})/2]$. Thus $\alpha \in \mathfrak{O}_D$. Furthermore $N(\alpha) = -1$. In order to apply Theorem 1 we have to determine when $\mathbb{Q}(\sqrt{P^2+4}) = \mathbb{Q}(\sqrt{2})$, that is we have to find all solutions P to the Pell equation $P^2 - 2Q^2 = -4$. The fundamental unit of $\mathbb{Q}(\sqrt{2})$ is $1 + \sqrt{2}$. By the theory of Pell equations it follows that the solutions $(P, Q) \in \mathbb{Z}^2_{\geq 0}$ of $P^2 - 2Q^2 = -4$ are precisely given by $\{(x_n, y_n) :\ n \geq 1 \text{ is odd }\}$, where $x_n + y_n\sqrt{2} = 2(1+\sqrt{2})^n$. Using induction it is easily proved that $x_n = L_n(2)$. Theorem 2 now follows on invoking Theorem 1. □

With the previous proof in mind the reader will have little problems in proving the following curiosum.

Theorem 4 *Let $D > 1$ be squarefree. Suppose that $X^2 - DY^2 = -4$ has a solution. Put, for $i = 1, 2$,*

$$C_i = \{P : P^2 - DQ^2 = (-1)^i 4 \text{ for some } Q \in \mathbb{Z}\}$$

and

$$C_{2+i} = \{Q : P^2 - DQ^2 = (-1)^i 4 \text{ for some } P \in \mathbb{Z}\}.$$

Then, when $D = 2$, $\delta(C_1) = 7/24$, $\delta(C_2) = 5/12$, $\delta(C_3) = 7/24$ and $\delta(C_4) = 17/24$. If $D > 2$, then $\delta(C_1) = 1/3$, $\delta(C_2) = 1/3$, $\delta(C_3) = 1/3$ and $\delta(C_4) = 2/3$.

The case $D = 2$

Table I.1

Prime density of the set
$\{p : \left(\frac{2}{p}\right) = 1,\ p \equiv 1 + 2^j (\bmod\ 2^{j+1}),\ 2^e \| \rho_\epsilon(p)\}$,
where $N(\epsilon) = -1$

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

Table I.2

Prime density of the set
$\{p : \left(\frac{2}{p}\right) = -1,\ p \equiv -1 + 2^j (\bmod\ 2^{j+1}),\ 2^e \| \rho_\epsilon(p)\}$,
where $N(\epsilon) = -1$

$e\backslash j$	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	$\frac{1}{4}$	0	0	0	0	0	...	$\frac{1}{4}$
3	0	0	0	0	0	0	0	...	0
4	0	0	0	0	0	0	0	...	0
5	0	0	0	0	0	0	0	...	0
6	0	0	0	0	0	0	0	...	0
...	...	...	...	...	...	...	...	...	...
	$\frac{1}{4}$	$\frac{1}{4}$	0	0	0	0	0	...	$\frac{1}{2}$

The case $D \neq 2$ and $N(\epsilon_D) = -1$

Table II.1

Prime density of the set
$\{p : \left(\frac{D}{p}\right) = 1,\ p \equiv 1 + 2^j (\mathrm{mod}\ 2^{j+1}),\ 2^e \| \rho_\epsilon(p)\}$,
where $N(\epsilon) = -1$

$e \backslash j$	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 II.2

Prime density of the set
$\{p : \left(\frac{D}{p}\right) = -1,\ p \equiv -1 + 2^j (\mathrm{mod}\ 2^{j+1}),\ 2^e \| \rho_\epsilon(p)\}$,
where $N(\epsilon) = -1$

$e \backslash j$	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] F. Halter-Koch, Arithmetische Theorie der Normalkörper von 2-Potenzgrad mit Diedergruppe, *J. Number Theory* **3** (1971), 412-443.

[3] 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.

[4] 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).

[5] P. Moree, Counting divisors of Lucas numbers, MPI-preprint, no. 34, Bonn, 1996.

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

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

[8] P. Stevenhagen, The number of real quadratic fields having units of negative norm, *Experimental Mathematics* **2** (1993), 121-136.

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

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