THE SET OF PRIMES DIVIDING THE LUCAS NUMBERS HAS DENSITY 2/3

J. C. Lagarias

Bell Laboratories
Murray Hill, NJ 07974

1. Introduction

There has been a good deal of study of the structure of the set of prime divisors of the terms $\{ U_n \}$ of second order linear recurrences. M. Ward [14] showed that there are always an infinite number of distinct primes dividing the terms $\{ U_n \}$, provided we exclude certain degenerate cases such as $U_n = 2^n$. In fact, under the same circumstances it is believed that the set of primes dividing the terms $U = \{ U_n \}$ of any nondegenerate second order linear recurrence has a positive density $d(U)$ depending on the recurrence. This can be proved under the asSption that the generalized Riemann hypothesis is true by a method analogous to Hooley's conditional proof of Artin's Conjecture for primitive roots. P. J. Stephens [13] has done this for a large class of such second-order recurrences.

The point of this paper is that there are special second order linear recurrences where it is possible to give an unconditional proof of the existence of a density. This was shown by Hasse [4] for certain special second order recurrences having a reducible characteristic polynomial, in the process of solving a problem of Sierpinski [12]. Sierpinski's problem concerns the existence of a density for the set of primes p for which $ord_p 2$ is even. This set of primes is exactly the set of primes dividing some term of the sequence $V_n = 2^n + 1$; this sequence satisfies the reducible second order linear recurrence $V_n = 3 V_{n-1} - 2 V_{n-2}$ with $V_0 = 2$ and $V_1 = 3$.

Theorem A. (Hasse) The set of primes $S_V = \{ p$: p is prime and p divides $2^n + 1$ for some $n \geq 0 \}$ has density 2/3.

Hasse's result [4] actually covers all the sequences $\{ a^n + 1 : \; n \geq 0 \}$, where a is an integer.

Here we observe that Hasse's method with some extra complications extends to cover certain second-order linear recurrences with irreducible characteristic polynomial. The most interesting example of this phenomonon is the Lucas numbers L_n defined by $L_1 = 2, L_2 = 1$ and the recurrence $L_{n+1} = L_n + L_{n-1}$.

Theorem B. The set of primes $S_L = \{p : p$ is prime and *p divides some Lucas number $L_n\}$ has density 2/3.*

Theorem B can be alternatively derived from polynomial-splitting criteria of M. Ward [16] for membership in S_L; this is essentially the same proof.

Hasse's method applies to any irreducible second-order recurrence $\{U_n\}$ whose general term can be written

$$U_n = \alpha\theta^n + \bar{\alpha}\bar{\theta}^n$$

where α and θ are in the quadratic field K generated by the roots of the characteristic polynomial of $\{U_n\}$, and $\bar{\alpha}$, $\bar{\theta}$ are the algebraic conjugates of α, θ in K, provided that:

(i) $\dfrac{\theta}{\bar{\theta}} = \pm\,\phi^k$ *where $k = 1$ or 2 for some ϕ in K.*

(ii) $\dfrac{\bar{\alpha}}{\alpha} = \zeta\phi^j$ *where ζ is a root of unity in K and j is an integer.*

The actual densities of the sets of primes obtained depend in an idiosyncratic way on α and θ, which makes it awkward to state a general result. Some of the possible extra complications encountered are illustrated in the proof of the following result, concerning a particular recurrence discussed in Laxton [8].

Theorem C. Let W_n denote the recurrence defined by $W_0 = 1$, $W_1 = 2$ and $W_n = 5W_{n-1} - 7W_{n-2}$. Then the set $S_W = \{p : p$ divides W_n for *some $n\}$ has density 5/8.*

The parameterized families of recurrences $A_n(m)$ and $B_n(m)$, both of which satisfy the recurrence

$$U_n = mU_{n-1} - U_{n-2}$$

with initial conditions $A_0(m) = B_0(m) = 1$ and $A_1(m) = m+1$, $B_1(m) = m-1$, are also recurrences to which Hasse's method applies. In the case that $\varepsilon = \frac{1}{2}(m + \sqrt{m^2-4})$ is the fundamental unit in $K = Q(\sqrt{m^2-4})$ the sets $S_A(m) = \{p : p$ *divides* $A_n(m)$ for *some* $n\}$ and $S_B(m) = \{p : p$ *divides* $B_n(m)$ for *some* $n\}$ each have density 1/3. I omit the details.

I give a proof of Theorem A in Section 2 for comparison with the more involved details of the proofs of

Theorem B and C in Sections 3 and 4, respectively.

2. Proof of Theorem A

The condition that $p \mid 2^n + 1$ for some n can be rewritten as:

$$2^n \equiv -1 \ (mod\ p) \ is\ solvable \ . \tag{2.1}$$

Now let $m = ord_p\ 2$, the least positive integer with

$$2^m \equiv 1 \ (mod\ p) \ . \tag{2.2}$$

Now (2.1) is solvable if and only if m is even and the smallest solution to (2.1) in that case is $n = \frac{1}{2} m$. Now suppose 2^j exactly divides $p-1$. Then we have:

$$2^j \ \| \ p-1 \text{ and } ord_p\ 2\ is\ odd \ \Leftrightarrow \ 2^{\frac{p-1}{2^j}} \equiv 1 \ (mod\ p) \ . \tag{2.3}$$

Hasse observes that the condition on the right side of (2.3) is a splitting condition for primes in a certain algebraic number field K_j; such sets of primes have a density by the Frobernius density theorem.

Consequently we proceed by decomposing the set S_V into disjoint sets

$$S_V = \bigcup_{j=1}^{\infty} S_V^{(j)} \tag{2.4}$$

given by

$$S_V^{(j)} = \{p\colon p \equiv 1 + 2^j \ (mod\ 2^{j+1}) \text{ and } p \ \varepsilon \ S_A\} \ .$$

We also define

$$\overline{S}_V^{(j)} = \{p\colon p \equiv 1 + 2^j \ (mod\ 2^{j+1}) \text{ and } p \notin S_A\} \ .$$

and observe $p \ \varepsilon \ \overline{S}_V^{(j)}$ if and only if $p \equiv 1 + 2^j \ (mod\ 2^{j+1})$ and (2.3) holds. To state Hasse's observation precisely, let C_j denote the cyclotomic field $Q(\sqrt[2^j]{1})$, let $K_j = Q(\sqrt[2^j]{1}, \sqrt[2^j]{2})$ and let $L_j = Q(\sqrt[2^{j+1}]{1}, \sqrt[2^j]{2})$.

Lemma 2.1. (1) The primes p in $\overline{S}_V^{(j)}$ are exactly the primes p that split completely in L_j but not in K_j.

(2) The primes p in $\overline{S}_V^{(j)}$ *have density* 2^{-2j} *and those in* $S_V^{(j)}$ *have density* $2^{-j} - 2^{-2j}$*, i.e.*

$$\# \{ p \le x \colon p \ \varepsilon \ \overline{S}_V^{(j)} \} \sim 2^{-2j} \ \frac{x}{lnx} \ ,$$

$$\# \{ p \le x \colon p \ \varepsilon \ S_V^{(j)} \} \sim (2^{-j} - 2^{-2j}) \ \frac{x}{lnx} \ ,$$

as $x \rightarrow \infty$.

Proof. The fields $C_j = Q(\sqrt[2^{j-1}]{-1})$, $K_j = C_j(\sqrt[2^j]{2})$ and $L_j = C_{j+1}(\sqrt[2^j]{2})$ are all normal extensions of the rationals. The condition that the ideal (p) split completely over a cyclotomic field $Q(\sqrt[m]{1})$ is well known to be $p \equiv 1 \ (mod \ m)$ ([2], Lemma 4), hence $p \equiv 1 \ (mod \ 2^j))$ holds if and only if p splits completely in C_j. The condition that a prime ideal p in C_j split completely in the Kummer extension $K_j = C_j(\sqrt[2^j]{2})$ is exactly that

$$x^{2^j} \equiv 2 \ (mod \ (p)) \ \text{ for } x \ \varepsilon \ O_j \tag{2.5}$$

be solvable over the ring of integers O_j for C_j ([2], Lemma 5). If p is of degree 1 then any algebraic integer x in C_j is congruent to a rational integer $(mod \ p)$ so in this case equation (2.5) is solvable if and only if

$$x^{2^j} \equiv 2 \ (mod \ p) \ \text{ for } x \ \varepsilon \ Z \tag{2.6}$$

is solvable. By Euler's criterion (2.6) is solvable if and only if

$$2^{\frac{p-1}{2^j}} \equiv 1 \ (mod \ p) \tag{2.7}$$

is solvable. This is exactly (2.3), and we have shown (p) splits completely in K_j *iff* $p \equiv 1 \ (mod \ 2^j)$ and (2.7) holds. Similarly (p) splits completely in L_j *iff* $p \equiv 1 \ (mod \ 2^{j+1})$ and (2.7) holds. This proves (1).

To prove (2) we observe that for a normal extension *K/Q* of degree $[K \colon Q]$ the set of primes p that split completely in K has density $[K \colon Q]^{-1}$, which is a consequence of the prime ideal theorem (e.g. [6], p. 315 Theorem 4), a special case of both the Frobenius and Chebotarev density theorem. Now $[C_j \colon Q] = 2^{j-1}$, $[K_j \colon Q] = 2^{2j-1}$ and $[L_j \colon Q] = 2^{2j}$. The set of primes in $\overline{S}_V^{(j)}$ is the difference of a set of primes of density $2^{-(2j-1)}$ less a class of primes contained in it of density 2^{-2j}, hence has density 2^{-2j}. Finally the primes in $S_V^{(j)}$ are the difference of the class of primes $\{ p \equiv 1 + 2^j \ (mod \ 2^{j+1}) \}$ of density $2^{-j} = [C_j \colon Q]^{-1} - [C_{j+1} \colon Q]^{-1}$, and the class of primes $\overline{S}_V^{(j)}$ of density 2^{-2j} contained in it. This proves

(2). ■

To complete the proof of Theorem A, we observe that for any fixed m,

$$\bigcup_{j=1}^{m} S_V^{(j)} \subseteq S_V \subseteq \mathbf{P} - \bigcup_{j=1}^{m} \overline{S}_V^{(j)}$$

where **P** denotes the set of all primes. Using (2) of Lemma 2.1, the first inclusion gives

$$\# \{p \le x\colon p \ \varepsilon \ S_V\} \ge \left(\frac{2}{3} - 2^{-m} - \frac{4}{3} 2^{-2m} \right) \frac{x}{lnx} + O\left(\frac{x}{lnx} \right)$$

as $x \to \infty$, since all the $S_V^{(j)}$ are disjoint. The second inclusion gives

$$\# \{p \le x\colon p \ \varepsilon \ S_V\} \le \left(\frac{2}{3} + \frac{4}{3} 2^{-2m} \right) \frac{x}{lnx} + O\left(\frac{x}{lnx} \right) .$$

as $x \to \infty$. Letting $m \to \infty$ shows that

$$\# \{p \le x\colon p \ \varepsilon \ S_V\} \sim \frac{2}{3} \frac{x}{lnx} .$$

Remarks. (1) By a careful analysis of error terms in this argument using an effective version of the Chebotanev density theorem, Odoni [11] has proved the stronger result that:

$$\# \{p \le x\colon p \ \varepsilon \ S_V\} = \frac{2}{3} Li(x) + O\left(Li(x) \ \exp(-c \frac{lnlnx}{lnlnlnx}) \right)$$

where $Li(x) = \int_2^x \frac{dt}{lnt}$.

(2) The sets $S_V^{(j)}$ are sets of primes determined by systems of polynomial congruences in the sense of [5, Theorems 1.1 and 1.2].

3. Proof of Theorem B

The Lucas numbers L_n satisfy

$$L_n = \varepsilon^n + \overline{\varepsilon}^n \tag{3.1}$$

where $\varepsilon = \frac{1+\sqrt{5}}{2}$ and $\overline{\varepsilon} = \frac{1-\sqrt{5}}{2}$. Hence

$$\begin{aligned} p|L_n &\iff \varepsilon^n + \varepsilon^{-1} \equiv \theta(mod\ (p)) \\ &\iff \theta^n \equiv -1\ (mod\ (p)) \end{aligned} \qquad (3.2)$$

where

$$\theta = \frac{\varepsilon}{\bar{\varepsilon}} = -\varepsilon^2 = -\frac{3+\sqrt{5}}{2}$$

and the congruences are in the ring $Z[\frac{1+\sqrt{5}}{2}]$ of algebraic integers in $Q(\sqrt{5})$. Thus S_L is exactly the set of primes p for which the exponential congruence over $Z[\frac{1+\sqrt{5}}{2}]$

$$\theta^x \equiv -1\ (mod\ (p)) \qquad (3.3)$$

is solvable for some integer *x*.

We now proceed analogously to the proof of Theorem A. We must treat several cases according to the behavior of the ideal (p) in $Z[\frac{1+\sqrt{5}}{2}]$. If $p \equiv \pm\ 1$ (mod 5) then $(p) = \pi\,\bar{\pi}$ splits into two conjugate degree 1 prime ideals, while if $p \equiv \pm\ 2\ (mod\ 5)$ then (p) is a degree 2 prime ideal in $Z[\frac{1+\sqrt{5}}{2}]$. Let $S_L = S_A \cup S_B$ where

$$S_A = \{p\colon p\ \varepsilon\ S_L \text{ and } p \equiv \pm 1\ (mod\ 5)\}$$

and

$$S_B = \{p\colon p\ \varepsilon\ S_L \text{ and } p \equiv \pm 2\ (mod\ 5)\}\ .$$

Case 1. The primes in S_A have density $\frac{5}{12}$.

Write $(p) = \pi\,\bar{\pi}$ in $Z[\frac{1+\sqrt{5}}{2}]$. In this case (3.3) is equivalent to

$$\theta^x \equiv -1\ (mod\ \pi_1) \qquad (3.4)$$

being solvable. To see this, suppose (3.4) holds and apply the automorphism taking $\sqrt{5}$ to $-\sqrt{5}$ to (3.4) to get

$$\bar{\theta}^{x} \equiv -1 \ (mod\ \bar{\pi}_1)\ . \tag{3.5}$$

Since $\theta\bar{\theta} = 1$ we have $\theta^x \bar{\theta}^x = 1$ so (3.5) implies

$$\theta^x \equiv -1 \ (mod\ \bar{\pi}_1)\ .$$

Combining this with (3.4) shows (3.3) holds. The reverse direction is clear.

Now we have the equivalence

$$ord_{\pi_1} \theta \ \mathit{is\ even} \ \Leftrightarrow \ \theta^x \equiv -1 \ (mod\ (p)) \ \mathit{is\ solvable}\ . \tag{3.6}$$

If $p \equiv 1 + 2^j \ (mod\ 2^{j+1})$ we obtain

$$2^j \ || \ p-1 \ \text{and} \ ord_{\pi} \theta \ \mathit{is\ odd} \ \Leftrightarrow \ \theta^{\frac{p-1}{2^j}} \equiv 1 \ (mod\ \pi_1)\ .$$

This leads us to split S_A into the disjoint union of sets

$$S_A = \bigcup_{j=1}^{\infty} S_A^{(j)} \ ,$$

where

$$S_A^{(j)} = \{p\colon p \equiv 1+2^j \ (mod\ 2^{j+1}) \ \text{and} \ ord_{\pi_1} \theta \ \mathit{is\ even}\}\ .$$

We set

$$\bar{S}_A^{(j)} = \{p\colon p \equiv 1+2^j \ (mod\ 2^{j+1}) \ \text{and} \ ord_{\pi_1} \theta \ \mathit{is\ odd}\}\ .$$

The associated fields are $K_j^* = Q(\sqrt[2^j]{1}, \sqrt{5}, \sqrt[2^j]{\theta})$ and $L_j^* = Q(\sqrt[2^{j+1}]{1}, \sqrt{5}, \sqrt[2^j]{\theta})$.

Lemma 3.1. (1) $\bar{S}_A^{(1)}$ is empty. For $j \geq 2$ the primes p in $\bar{S}_A^{(j)}$ are exactly the primes that split completely in K_j^* and which do not split completely in L_j^*.

(2) The primes in $\bar{S}_A^{(1)}$ and $S_A^{(1)}$ have densities 0 and 1/4, respectively. For $j \geq 2$ the primes in $\bar{S}_A^{(j)}$ have density 2^{-2j} and those in $S_A^{(j)}$ have density $2^{-j-1} - 2^{-2j}$.

Proof. Similar to that of Lemma 2.1. The relation $\theta = -\varepsilon^2$ leads to $K_1^* = L_1^* = Q(\sqrt{-1}, \sqrt{5})$; this causes $S_A^{(1)}$ to be empty. For $j \geq 2$ one checks that $[K_j^*\colon Q] = 2^{2j-1}$ and $[L_j^*\colon Q] = 2^{2j}$. In fact for $j \geq 2$, $K_j^* = Q(\omega_j, \sqrt{5}, \phi_{j-2}\sqrt{\omega_j \phi_{j-2}})$ where $\omega_j = \sqrt[2^{j-1}]{-1}$ and $\phi_{j-2} = \sqrt[2^{j-2}]{\varepsilon},$ and

$L_j^* = Q(\omega_{j+1}, \sqrt{5}, \phi_{j-1})$. Finally note that the set $S_A^{(j)} \cup \overline{S}_A^{(j)} = \{p: p \equiv \pm 1 \ (mod\ 5)\}$ and $p \equiv 1+2^j \ (mod\ 2^{j+1})$ has density 2^{-j-1}. ■

As in the proof of Theorem A we find the primes in S_A have density $\frac{1}{4} + \sum_{j=2}^{\infty} (2^{-j+1} - 2^{-2j}) = \frac{1}{2} - \frac{1}{12} = \frac{5}{12}$.

Case 2. The primes in S_B have density $\frac{1}{4}$.

The primes $p \equiv \pm 2 \ (mod\ 5)$ remain inert in $Z[\frac{1+\sqrt{5}}{2}]$, and in this case

$$\theta^x \equiv -1 \ (mod\ (p)) \ \textit{is solvable} \ \Leftrightarrow \ ord_{(p)}\theta \ \textit{is even} .$$

Now

$$\theta^{\frac{p+1}{2}} = (-1)^{\frac{p+1}{2}} \varepsilon^{p+1} \equiv a \ (mod\ p)$$

for some $a \in Z$ because $GF(p)^* = \{\psi^{p+1}: \psi \in GF(p^2)^*\}$. Applying the nontrival automorphism of $Q(\sqrt{5})$ gives

$$\overline{\theta}^{\frac{p+1}{2}} \equiv a \ (mod\ p)$$

hence

$$1 = (\theta\overline{\theta})^{\frac{p+1}{2}} \equiv a^2 \ (mod\ (p)) \ .$$

Thus

$$\theta^{p+1} \equiv a^2 \equiv 1 \ (mod\ (p)) \tag{3.8}$$

Consequently $ord_{(p)}\theta \mid p+1$. Now when $p \equiv -1+2^j \ (mod\ 2^{j+1})$ we have

$$\theta^{\frac{p+1}{2^j}} \equiv 1 \ (mod\ (p)) \ \Leftrightarrow \ ord_{(p)}\theta \ \textit{is odd} . \tag{3.9}$$

We now decompose

$$S_B = \bigcup_{j=1}^{\infty} S_B^{(j)}$$

where

$$S_B^{(1)} = \{p\colon p \equiv 1\ (mod\ 4) \text{ and } p\ \varepsilon\ S_B\}\ .$$

and

$$S_B^{(j)} = \{p\colon p \equiv -1+2^j\ (mod\ 2^{j+1}) \text{ and } p\ \varepsilon\ S_B\}\ .$$

We complete case 2 with the following lemma.

Lemma 3.2. (1) $S_B^{(1)}$ is empty.

(2) For $j \geq 2$ all $S_B^{(j)} = \{p\colon p \equiv -1+2^j\ (mod\ 2^{j+1})$ and $p \equiv \pm 2\ (mod\ 5)\}$ and $S_B^{(j)}$ has density 2^{-j}.

Proof. (1) When $j=1$ we have

$$\theta^{\frac{p+1}{2}} \equiv 1\ (mod\ (p)) \iff ord_{(p)}\theta\ is\ odd\ . \tag{3.10}$$

Now $\theta = -\varepsilon^2$ so

$$\theta^{\frac{p+1}{2}} \equiv (-\varepsilon^2)^{\frac{p+1}{2}} \equiv -\varepsilon^{p+1}\ (mod\ (p))\ , \tag{3.11}$$

We claim

$$\varepsilon^{p+1} \equiv -1\ (mod\ (p))$$

which with (3.11) shows $\theta^{\frac{p+1}{2}} \equiv 1\ (mod\ (p))$ and so by (3.10) $ord_p \theta$ is odd and $S_B^{(1)}$ is empty.

To prove the claim, set

$$\varepsilon^{\frac{p+1}{2}} \equiv \phi\ (mod\ (p))$$

so

$$\varepsilon^{p+1} \equiv \phi^2\ (mod\ (p))\ . \tag{3.12}$$

By conjugation $\bar{\varepsilon}^{\frac{p+1}{2}} \equiv \bar{\phi}\ (mod\ p)$ and $\varepsilon\bar{\varepsilon} = -1$ so that

$$-1 = (-1)^{\frac{p+1}{2}} \equiv (\varepsilon\bar{\varepsilon})^{\frac{p+1}{2}} \equiv \phi\bar{\phi} \ (mod\ (p)) \ . \tag{3.13}$$

By (3.8) $\varepsilon^{p+1} \equiv \pm 1 \ (mod\ (p))$. We suppose $\varepsilon^{p+1} \equiv 1 \ (mod\ (p))$ and get a contradiction. In that case (3.12) gives $\phi^2 \equiv 1 \ (mod\ (p))$, hence $\phi \equiv \pm 1 \ (mod\ (p))$. Hence $\phi \equiv \bar{\phi} \ (mod\ (p))$ and (3.13) now gives

$$\phi^2 \equiv -1 \ (mod\ (p)) \ ,$$

the desired contradiction.

(2) We must show that in the case $j \geq 2$ for any $p \equiv -1+2^j \ (mod\ 2^{j+1})$ and $p \equiv \pm 2 \ (mod\ 5)$ we claim $ord_{(p)}\theta$ is even. We argue by contradiction. Suppose $ord_{(p)}\theta$ were odd, so that by (3.8) we have

$$\theta^{\frac{p+1}{2^j}} \equiv 1 \ (mod\ (p)) \tag{3.14}$$

Set

$$\varepsilon^{\frac{p+1}{2^j}} \equiv \phi \ (mod\ (p))$$

and observe (3.14) gives

$$-\phi^2 \equiv 1 \ (mod\ (p)) \ . \tag{3.15}$$

Now

$$\bar{\varepsilon}^{\frac{p+1}{2^j}} \equiv \bar{\phi} \ (mod\ (p))$$

and

$$-1 = (-1)^{\frac{p+1}{2^j}} \equiv (\varepsilon\bar{\varepsilon})^{\frac{p+1}{2^j}} \equiv \phi\bar{\phi} \ (mod\ (p)) \ . \tag{3.16}$$

Now by (3.15) $\phi^2 \equiv -1 \ (mod\ (p))$ and since $p \equiv 3 \ (mod\ 4)$ $\bar{\phi} \equiv -\phi \ (mod\ (p))$. Hence $\phi\bar{\phi} \equiv -\phi^2 \equiv 1 \ (mod\ (p))$, contradicting (3.16). ■

As in the proof of Theorem A Lemma 3.2 implies the density of primes in S_B is $\sum_{j=2}^{\infty} 2^{-j-1} = \frac{1}{4}$. This proves Theorem B. ■

4. Proof of Theorem C (Sketch)

We have

$$V_n = \left(\frac{1}{2} + \frac{1}{6}\sqrt{-3}\right)\left(\frac{5}{2} + \frac{1}{2}\sqrt{-3}\right)^n + \left(\frac{1}{2} - \frac{1}{6}\sqrt{-3}\right)\left(\frac{5}{2} - \frac{1}{2}\sqrt{-3}\right)^n . \qquad (4.1)$$

Letting $\alpha = \frac{1}{2} + \frac{1}{6}\sqrt{-3}$ and $\gamma = \frac{5}{2} + \frac{1}{2}\sqrt{-3}$ we have

$$V_n \equiv 0 (mod\ (p)) \iff \phi^n \equiv -\frac{\bar{\alpha}}{\alpha}\ (mod\ (p)) , \qquad (4.2)$$

where $\phi = \frac{\gamma}{\bar{\gamma}} = \frac{11+5\sqrt{-3}}{14}$ and $-\frac{\bar{\alpha}}{\alpha} = \frac{-1+\sqrt{-3}}{2}$ is a cube root of unity. Hence (4.1) gives

$$p\ divides\ V_n \text{ for } some\ n \geq 0 \iff ord_{(p)}\ \phi \equiv 0\ (mod\ 3) . \qquad (4.3)$$

We consider separately the cases in which (p) splits completely or remains inert in $Q(\sqrt{-3})$.

Case 1. $p \equiv 1\ (mod\ 3)$.

Then $(p) = \pi\bar{\pi}$ in $Z[\frac{1+\sqrt{-3}}{2}]$. Now as in Theorem B we have

$$ord_{(p)}\ \phi \equiv 0\ (mod\ 3) \iff ord_{\pi}\ \phi \equiv 0\ (mod\ 3), \qquad (4.4)$$

using the fact that $\phi\bar{\phi} = 1$. Now let $3^j || p-1$, and observe that in this case

$$ord_{\pi}\ \phi \not\equiv 0\ (mod\ 3) \iff \phi^{\frac{p-1}{3^j}} \equiv 1\ (mod\ \pi) \qquad (4.5)$$

Then

$$\theta^{\frac{p-1}{3^j}} \equiv 1\ (mod\ \bar{\pi}) \iff \pi\ splits\ completely\ in\ F_j = Q(\sqrt[3^j]{1}, \sqrt[3^j]{\theta})/Q(\sqrt[3]{1})$$

$$\iff (p)\ splits\ completely\ in\ F_j/Q . \qquad (4.6)$$

Hence the density of primes satisfying (4.6) is $[F_j : Q]^{-1} = (2 \cdot 3^{2j-1})^{-1}$, and the density d_j of primes with $3^j || p-1$ and (4.4) holding is

$$d_j = 2(2 \cdot 3^j)^{-1} - (2 \cdot 3^{2j-1})^{-1}$$

The total contribution of such primes has density

$$D_1 = \sum_{j=1}^{\infty} d_j = \frac{5}{16} . \tag{4.7}$$

Case 2. $p \equiv 2 \ (mod\ 3)$.

Then (p) is inert in $Z[\frac{1+\sqrt{-3}}{2}]$ and, as in Theorem B we have

$$\phi^{p+1} \equiv 1 \ (mod\ (p))$$

and if $3^j \,||\, p+1$ then

$$ord_{(p)}\ \phi \neq 0 \ (mod\ 3) \ \Leftrightarrow \ \phi^{\frac{p+1}{3^j}} \equiv 1 \ (mod\ (p)) \ .$$

Now we have

$$\phi^{\frac{p+1}{3^j}} \equiv 1 \ (mod\ (p)) \ \Leftrightarrow \ p \equiv 2 \ (mod\ 3) \text{ and } (p) \textit{ splits completely in } F_j/Q(\sqrt{-3}\,) \tag{4.8}$$

We claim that the set of primes defined by the right side of (4.9) has density $(2 \cdot 3^{2j-1})^{-1}$. To verify this, one checks that F_j/Q is Galois over Q with Galois group of order $2 \cdot 3^{2j-1}$, that the splitting condition (4.8) on primes in F_j/Q corresponds exactly to the Artin symbol $[\frac{F_j/Q}{(p)}]$ being the conjugacy class $<\sigma>$, where σ is the unique element of order two in Gal (F_j/Q). Then the Chebotarev density theorem implies that the set of primes in (4.8) has density $[F_j:Q]^{-1} = (2 \cdot 3^{2j-1})^{-1}$, as claimed.

Hence the density d_j^* of primes with $3^j \,||\, p+1$ and (4.4) holding is

$$d_j^* = 2(2 \cdot 3^j)^{-1} - (2 \cdot 3^{2j-1})^{-1}$$

and the total density of such primes is

$$D_2 = \sum_{j=1}^{\infty} d_j^* = \frac{5}{16} . \ \blacksquare$$

Acknowledgement

I am indebted to J. P. Serre for informing me of the work of Hasse.

References

[1] A. Aigner, Bemerkung und Lösung zum Problem 29, Elem d. Math. *15* (1960), 66-67.

[2] B. J. Birch, Cyclotomic Fields and Kummer Extensions, in: *Algebraic Number Fields* (J. W. S. Cassels and A. Fröhlich, Eds.), Academic Press, London 1967, 85-93.

[3] H. Hasse, Über die Dichte der Primzahlen p, fur die vorgegebene ganzrationale Zahl $a \neq 0$ von durch eine vorgegebene Primzahl ➳ ≠ 2 teilbarer bzw. unteilbarer Ordnung mod p ist., Math. Ann. *162* (1965), 74-76.

[4] 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. Annalen *166* (1966) 19-23.

[5] J. C. Lagarias, Sets of primes determined by systems of polynomial congruences, Illinois J. Math. *27* (1983), 224-235.

[6] S. Lang, *Algebraic Number Theory*, Addison-Wesley Publ. Co., New York 1970.

[7] R. R. Laxton, On groups of linear recurrences I, Duke Math J. *26* (1969) 721-736.

[8] R. R. Laxton, On groups of linear recurrences II. Elements of Finite Order, Pacific J. Math. *32* (1970) 173-179.

[9] R. R. Laxton, Arithmetic Properties of Linear Recurrences, in: Computers and Number Theory (A. O. L. Atkin and B. J. Birch, Eds.), 119-124.

[10] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, Polish Scientific Publishers, Warsaw 1974.

[11] R. W. K. Odoni, A Conjecture of Krishnamurthy on Decimal Periods and Some Allied Problems, J. Number Theory 13 (1981) 303-319.

[12] W. Sierpinski, Sur une decomposition des numbers premiers en deux classes, Collect. Math. *10* (1958), 81-83. (Also: Problem 29, Elem. d. Math. *14* (1959), 60.)

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

[14] P. J. Stephens, Prime divisors of second order linear recurrences II, J. Number Theory 8 (1976), 333-345.

[15] M. Ward, Prime divisors of second order recurring sequences, Duke Math. J. *21* (1954), 178-188.

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

THE SET OF PRIMES DIVIDING THE LUCAS NUMBERS HAS DENSITY 2/3

J. C. Lagarias

Bell Laboratories
Murray Hill, NJ 07974

ABSTRACT

Dedicated to the memory of Ernst Straus

The Lucas numbers L_n are defined by $L_0 = 2$, $L_1 = 1$ and the recurrence $L_n = L_{n-1} + L_{n-2}$. The set of primes $S_L = \{p \colon p$ divides L_n for some $n\}$ has density 2/3. Similar density results are proved for sets of primes $S_U = \{p \colon p$ divides U_n for some $n\}$ for certain other special second-order linear recurrences $\{U_n\}$. The proofs use a method of Hasse.