ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 29, Number 3, Fall 1999

THE DENSITY OF PRIMES P, SUCH THAT -1 IS A RESIDUE MODULO P OF TWO CONSECUTIVE FIBONACCI NUMBERS, IS $2/3$

CHRISTIAN BALLOT

ABSTRACT. Given $\eta_1, \eta_2 \in \{\pm 1\}$, we calculate the exact proportion of primes p such that η_1, η_2 appear consecutively as residues of the Fibonacci sequence modulo p.

Introduction. Let $\eta_1, \eta_2 \in \{\pm 1\}$. In this paper we compute the density of the set of primes p such that η_1, η_2 appear as consecutive residues of the Fibonacci sequence (F_n) modulo p, i.e., such that there exists $n \in \mathbf{N} : (F_n, F_{n+1}) \equiv (\eta_1, \eta_2) \pmod{p}$.

The method used originated with Hasse, but its scope was later extended by Lagarias, and then Ballot. Let $U = (U_n)_{n \geq 0}$ be a linear recurrence sequence with integral terms and characteristic polynomial $f(X) \in \mathbf{Z}[X]$. Hasse [**6**] showed that for binary recurrence sequences $U_n = a^n + 1$, $a \in \mathbf{Z}$, one could compute the precise density of primes p such that p divides U, i.e., such that there exists $n \in \mathbf{N}$, $p \mid U_n$. Lagarias [**7**] went further by proving that Hasse's method applied to some binary linear recurrence sequences whose characteristic polynomials had *irrational* roots, in particular, to $U_n = L_n$, the sequence of Lucas numbers. The present author [**1**] discovered that one could generalize the method to the computing of densities of prime divisors of some linear recurrence sequences of arbitrary order $m \geq 2$ as long as one defined division of U to mean p divides $m - 1$ consecutive terms of the sequence U. (We then say that p is a *maximal divisor of* U.) However, all sequences of order $m \geq 3$ to which the method was applied in the author's memoir [**1**] had characteristic polynomials with rational roots. Here, for the first time, we deal with a *ternary* recurrence sequence whose characteristic polynomial, namely $f(X) = (X - 1)(X^2 - X - 1)$, has some *irrational* roots. Thus, we

Received by the editors on July 31, 1997.
1991 AMS *Mathematics Subject Classification.* Primary 11B37, 11B83, 11B05. Secondary 11B39.
Key words and phrases. Recurrence sequences, density, maximal division, Fibonacci residues.

enlarge the scope of Hasse's method somewhat further. Moreover, the ternary sequence treated, namely $1 + F_n$, is of noticeable interest since it is a simple translate of the Fibonacci sequence.

Section 1 is a short preliminary section in which we recall relevant definitions and introduce notation. Section 2 is the core of the paper where the density result announced in the title is computed. The proof proposed uses basic algebraic number theoretic concepts. Readers who wish to have the precise statements of the Kummer-Dedekind and Kronecker density theorem can find those in Appendix A of [**1**]. In Section 3, we reinterpret our result to obtain a theorem on the proportion of primes for which the pair (η_1, η_2) appears as consecutive residues of the Fibonacci sequence modulo p, for η_1, η_2 in $\{\pm 1\}$. Section 4 is reserved for an alternate proof of Theorem 3 of Section 2. This proof is of interest because it relies only on elementary Lucas theory. Sections 5 and 6 put the results of Sections 2 and 3 in relation to earlier work and in particular in relation to the theory developed about the Laxton-Ballot group (Section 5), but also to work about the prime divisors of the Lucas numbers by Ward and by Lagarias (Section 6). These last two sections actually show why the study of the prime divisors of the Lucas numbers and the study of the primes for which -1 is two consecutive times a residue of the Fibonacci numbers are intricately related questions. In fact, we do compare these two sets of primes (Theorem 9). Finally we show that some computational techniques given by Ward for deciding on whether a prime p divides the Lucas numbers are also relevant for deciding whether -1 appears as consecutive Fibonacci residues (end of Section 6).

It is worth mentioning that the density computation made and the techniques used in the paper, although we voluntarily limited our study to the sequence $1 + F$, readily apply to other ternary recurrences (of a similar kind). We suggest, for further study, a class of such sequences in the very last remark of Section 5.

1. Preliminaries.

Definitions. We say that a condition is verified for essentially all primes if it is true for all but possibly finitely many of the primes considered. That finitely many primes do not verify some statement

has no effect on the density results being proven, so we may occasionally not mention explicitly those exceptional primes. The densities we calculate are Dirichlet densities. Yet the sets of primes we consider have Dirichlet and natural densities which coincide (some information about the relationship between those two kinds of densities can be found in Serre's book [**9**, p. 76]. Here the natural density of a set S of primes is

$$d(S) = \lim \frac{\log x}{x} \cdot |\{p \in S : p \leq x\}|.$$

If U is a linear recurrence sequence of order $m \geq 2$ and p is a prime, then we say that p is a *maximal* divisor of U if it divides some $m-1$ consecutive terms of U. We write $p|_{\max}U$ to denote this fact. More precisely, p divides U maximally at n will mean that $p|u_n, p|u_{n+1}, \ldots, p|u_{n+m-2}$. (The standard definition of maximal division requires division of $m-1$ consecutive terms, but of no m consecutive terms. If a prime divides m consecutive terms of U, then it is a *null* divisor of U, i.e., one such that there exists k, for all $n \geq k$, $p|u_n$. But, for any linear recurrence sequence, the prime null divisors are always finitely many, see [**1**, Corollary 5.4.12]. For our purpose this slightly modified definition of maximal division is well-suited.)

Notation. We denote the algebraic conjugate of a quadratic irrational number x by $\bar{x}$. The symbol ζ_k represents a primitive kth root of unity. The golden ratio $(1+\sqrt{5})/2$ is denoted by ε. If p is a prime, then (p) represents the ideal generated by p, in $\mathbf{Z}$ or in the ring of integers $\mathbf{Z}[\varepsilon]$ of $\mathbf{Q}(\sqrt{5})$, or again in the ring of integers of the root field considered, depending on the context. Throughout Section 2, the symbol U designates the sequence $1 + F$, where F is the Fibonacci sequence defined by $F_0 = 0$, $F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$, for all $n \geq 0$. In Sections 4 and 5, we assume familiarity with the notions of a Lucas sequence and of a rank of a prime in such a sequence.

Finally, $\mathcal{P}$ denotes the set of all rational primes, $P(U)$ and $P_{\max}(U)$ the sets of prime divisors and prime maximal divisors of a sequence U, while $\delta(P)$ represents the density of the set of primes in P, if this density exists.

2. The density computation.

Lemma 1. *For essentially all primes p, we have*

(1) *p divides U maximally* $\iff \exists n \in \mathbf{N} : -1 \equiv \varepsilon^n \equiv \bar{\varepsilon}^n \pmod{(p)}$.

Proof. The classical identity

$$\varepsilon^{n+1} = \varepsilon \cdot F_{n+1} + F_n \tag{2}$$

is easily shown by induction. Now suppose p divides $(1+F_n)$ maximally at n, i.e. $F_n \equiv F_{n+1} \equiv -1 \pmod{p}$. Then, by (2), $\varepsilon^{n+1} \equiv -\varepsilon - 1 = -\varepsilon^2 \pmod{(p)}$, which implies $\varepsilon^{n-1} \equiv -1 \pmod{(p)}$, and by conjugation, $\bar{\varepsilon}^{n-1} \equiv -1 \pmod{(p)}$. The converse, i.e., $-1 \equiv \varepsilon^{n-1} \equiv \bar{\varepsilon}^{n-1} \pmod{(p)} \Longrightarrow F_n \equiv F_{n+1} \equiv -1 \pmod{p}$, is a direct verification having $F_n = (\varepsilon^n - \bar{\varepsilon}^n)/(\varepsilon - \bar{\varepsilon})$, $\forall\, n \geq 0$. □

Notation. Let Π be a prime ideal in $\mathbf{Z}[\varepsilon]$ lying above p. The order of ε modulo Π is denoted by e.

Lemma 2. *Let $p \in \mathcal{P}\backslash\{2,5\}$ and Π be a prime ideal in $\mathbf{Z}[\varepsilon]$ lying above p. Then*

$$p \mid_{max} U \iff 4 \mid e.$$

Proof. Note first that the condition for maximal division given in (1) is equivalent to

$$\exists n \in \mathbf{N} : \ -1 \equiv \varepsilon^n \equiv \bar{\varepsilon}^n \pmod{\Pi}. \tag{3}$$

This is plain if p is inert, since then $(p) = \Pi$. Now, if p splits then $(p) \subset \Pi$ and so (3) is necessary. To show sufficiency of (3), we conjugate (3) to obtain $-1 \equiv \varepsilon^n \equiv \bar{\varepsilon}^n \pmod{\bar{\Pi}}$ so that, since $(p) = \Pi \cap \bar{\Pi}$, (1) is true.

Note that the exponent n in (3) is necessarily even, since (3) $\Longrightarrow 1 = (-1)^2 \equiv \varepsilon^n \cdot \bar{\varepsilon}^n = (\varepsilon\bar{\varepsilon})^n = (-1)^n \pmod{\Pi}$ and $p \neq 2$. Hence, there exists $m \in \mathbf{N} : \varepsilon^{2m} \equiv -1 \pmod{\Pi} \Longrightarrow e|4m$ and $e \nmid 2m \Longrightarrow 4|e$.

Conversely, $4|e \Longrightarrow$ there exists $m \in \mathbf{N} : \varepsilon^{2m} \equiv -1 \pmod{\Pi}$. But $\varepsilon\bar{\varepsilon} = -1 \Longrightarrow \varepsilon^{2m}\bar{\varepsilon}^{2m} = 1$, which implies $\varepsilon^{2m}\bar{\varepsilon}^{2m} \equiv 1 \pmod{\Pi}$. So $\varepsilon^{2m} \equiv -1 \pmod{\Pi} \Longrightarrow \bar{\varepsilon}^{2m} \equiv -1 \pmod{\Pi}$. Hence (3) is satisfied for $n = 2m$. □

Theorem 3. *Essentially all primes congruent to* $\pm 2 \pmod 5$ *are maximal divisors of* U.

Proof. The primes congruent to ± 2 modulo 5 are inert in $\mathbf{Z}[\varepsilon]$ so that the Frobenius automorphism $\sigma = \sigma(p)$ is the nontrivial automorphism of $\mathbf{Q}(\sqrt{5})$ over $\mathbf{Q}$. That is, for all $x \in \mathbf{Z}[\varepsilon]$, we have $\bar{x} = \sigma(x) \equiv x^p \pmod{\Pi}$. Thus, $-1 = \varepsilon\bar{\varepsilon} = \varepsilon\sigma(\varepsilon) \equiv \varepsilon^{p+1} \pmod{\Pi}$. So, $e|2(p+1)$ and $e \nmid p+1$. Hence, $4 \mid e$ and $p|_{\max}U$ by Lemma 2. □

Theorem 4. *The primes congruent to* ± 1 *modulo* 5 *and dividing* U *maximally have density* $\delta = 1/6$.

Proof. For $j \geq 1$, let $S^j = \{p : p \equiv \pm 1 \pmod 5 \text{ and } p \equiv 1 + 2^j \pmod{2^{j+1}}\}$.

Let $j \geq 1$ and $p \in S^j$. Then, by Lemma 2, we have $p \nmid_{\max} U \Longleftrightarrow 4 \nmid e$.

But since p splits in $\mathbf{Z}[\varepsilon]$, the field $\mathbf{Z}[\varepsilon]/\Pi$ is isomorphic to $\mathbf{Z}/(p)$ and so $e|p-1$. Hence, $4 \nmid e \Longleftrightarrow \varepsilon^{(p-1)/2^{j-1}} \equiv 1 \pmod{\Pi}$, which by Euler's criterion means that $X^{2^{j-1}} - \varepsilon \equiv 0 \pmod{\Pi}$ is solvable in $\mathbf{Z}[\varepsilon]$. Now by the Kummer-Dedekind theorem, and if we bear in mind that $p \in S^j$, then the condition that $X^{2^{j-1}} - \varepsilon \equiv 0 \pmod{\Pi}$ be solvable in $\mathbf{Z}[\varepsilon]$ is equivalent to

$$\begin{aligned} &p \text{ splits completely in } F_j = \mathbf{Q}(\sqrt[2^{j-1}]{\varepsilon}, \zeta_{2^j}), \\ &\text{but not in } G_j = F_j(\zeta_{2^{j+1}}). \end{aligned} \tag{4}$$

Now F_j and G_j are normal extensions of $\mathbf{Q}$. Indeed, to see that F_j is normal, note that the minimal polynomial of $\alpha = \sqrt[2^{j-1}]{\varepsilon}$ is $(X^2)^{2^{j-1}} - X^{2^{j-1}} - 1$. The 2^j conjugates of α are of the form $\rho\alpha$ or $\rho\beta$, where ρ is any 2^{j-1}-th root of 1 and $\beta = \sqrt[2^{j-1}]{\bar{\varepsilon}}$. Note that $\alpha\beta = \zeta_{2^j} \in F_j \Longrightarrow \beta \in F_j$, so that all the conjugates of α are in F_j.

But F_j is the field obtained by adjoining all the conjugates of α to $\mathbf{Q}$. Hence, F_j is the splitting field of $X^{2^j} - X^{2^{j-1}} - 1$ and so is a normal extension of $\mathbf{Q}$.

But applying the Kronecker density theorem to (4), one gets the density $\bar{\delta}_j$ of primes in S^j which are not maximal divisors of U

$$\begin{aligned}\bar{\delta}_j &= \frac{1}{[F_j : \mathbf{Q}]} - \frac{1}{[G_j : \mathbf{Q}]} = \frac{1}{2} \cdot \frac{1}{[F_j : \mathbf{Q}]} \\ &= \frac{1}{2} \cdot \frac{1}{2^j \cdot 2^{j-1}} = \frac{1}{4^j}.\end{aligned}$$

Hence, because the sets S^j are disjoint, the density $\bar{\delta}$ of non-divisors among primes congruent to $\pm 1 \pmod 5$ is

$$\bar{\delta} = \sum_{j \geq 1} \bar{\delta}_j = \frac{1}{4} \cdot \frac{1}{1 - 1/4} = \frac{1}{3}.$$

And the density δ is then obtained by subtracting $\bar{\delta} = 1/3$ from the density of primes congruent to $\pm 1 \pmod 5$, i.e., $1/2$. Hence,

$$\delta = \frac{1}{2} - \frac{1}{3} = \frac{1}{6}. \qquad \square$$

Theorem 5. *The density of prime maximal divisors of* $(1 + F_n)$ *is* $2/3$.

Proof. It is a straightforward consequence of Theorem 3 and Theorem 4. $\square$

Numerical data. We found that 670 of the first thousand primes divide two consecutive terms of the sequence $1+F_n$. This data compares favorably to the density result of Theorem 5.

Remark. Note that all prime maximal divisors of U congruent to ± 1 modulo 5 must also be congruent to 1 modulo 4, since $4 \mid e \Longrightarrow 4 \mid p-1$. Hence we may summarize our density result by stating that the set of

maximal divisors of $U = 1 + F$ consists of the primes $\equiv \pm 2 \pmod 5$ and two-thirds of the primes $\equiv 1$ or $9 \pmod{20}$.

3. Consecutive ± 1 residues in the Fibonacci sequence.

Theorem 6. *The pairs* $(1,1)$ *and* $(-1,1)$ *are consecutive Fibonacci residues for all primes, while the pairs* $(-1,-1)$ *and* $(1,-1)$ *both occur as consecutive Fibonacci residues for the same set of primes*; *this set has density* $2/3$.

Proof. That there exists $n \in \mathbf{N} : (F_n, F_{n+1}) \equiv (1,1) \pmod p$, for all p prime, is indisputable since $(F_1, F_2) = (1,1)$. Similarly, we have $(F_{-2}, F_{-1}) = (-1,1)$ and because the Fibonacci sequence is periodic modulo p, the pair of residues $(-1,1)$ will occur as (F_n, F_{n+1}) modulo p with some $n \geq 0$ for any prime p.

Finally because $F_{n+2} \equiv F_{n+1} + F_n \pmod p$, one can readily verify that

$$(F_{n-2}, F_{n-1}) \equiv (1,-1) \pmod p \iff (F_{n+1}, F_{n+2}) \equiv (-1,-1) \pmod p,$$

so that $(1,-1)$ will occur as consecutive Fibonacci residues if and only if $(-1,1)$ does. The result then follows from Theorem 5. □

4. An elementary proof of Theorem 3. It is possible to give a proof of Theorem 3 which does not make use of the Frobenius automorphism and which is almost solely based on elementary Lucas identities. To present such a proof, we first state a result, which is a generalization of the usual Euler's criterion.

Proposition 7. (Euler's criterion for Lucas sequences). *Let* U *be the Lucas sequence associated to the quadratic polynomial* $X^2 - PX + Q$ *of discriminant* D. *If* $p \nmid 2QD$, *then*

$$p \mid U_{(p-\nu)/2} \iff \left(\frac{Q}{p}\right) = 1,$$

where ν *is the Legendre symbol* (D/p).

Proof. See [**3**, p. 628] or [**4**, p. 185]. These proofs rely on appropriate Lucas identities. □

Second proof of Theorem 3. Let p be a prime inert in $\mathbf{Z}[\varepsilon]$. From elementary Lucas theory, we know that $\varepsilon^{p+1} \equiv \bar{\varepsilon}^{p+1} \pmod{(p)}$, since then the rank of p in the Fibonacci sequence must divide $p+1$. Hence,

$$\left(\frac{\varepsilon}{\bar{\varepsilon}}\right)^{(p+1)/2} \equiv \pm 1 \pmod{(p)}. \tag{5}$$

The sign in (5) is given by Euler's criterion. Indeed, it is positive $\iff \varepsilon^{(p+1)/2} \equiv \bar{\varepsilon}^{(p+1)/2} \pmod{(p)} \iff p \mid F_{(p+1)/2}$ if and only if, by Proposition 7 and assuming $p \neq 2$, $(-1/p) = +1 \iff p \equiv 1 \pmod 4$. So in (5) we have respectively ± 1 according to whether $p \equiv \pm 1 \pmod 4$.

Now,

$$\begin{aligned}\left(\frac{\varepsilon}{\bar{\varepsilon}}\right)^{(p+1)/2} &= (-\varepsilon^2)^{(p+1)/2} = -(-1)^{(p-1)/2}\varepsilon^{p+1} \\ &= -\left(\frac{-1}{p}\right)\varepsilon^{p+1} \Longrightarrow \varepsilon^{p+1} = -\left(\frac{-1}{p}\right)\left(\frac{\varepsilon}{\bar{\varepsilon}}\right)^{(p+1)/2}.\end{aligned}$$

Hence,

$$\pmod{(p)}, \quad \varepsilon^{p+1} \equiv -1 \equiv \begin{cases} -(+1)(+1) & \text{if } p \equiv 1 \pmod 4, \\ -(-1)(-1) & \text{if } p \equiv -1 \pmod 4. \end{cases}$$

So $\varepsilon^{p+1} \equiv -1 \pmod{(p)}$, for essentially any inert prime p. Consequently, $-1 \equiv \varepsilon^{p+1} \equiv \bar{\varepsilon}^{p+1} \pmod{(p)}$ which, by Lemma 1, means that p is a maximal divisor of $(1 + F_n)$. □

5. Relation between $1 + F_n$ and the Laxton-Ballot group. Omitting some technicalities, we will say that Laxton [**8**] constructed a group structure on the set of all sequences of integers that satisfy the same binary recurrence. The group operation $*$ is such that if a prime p divides both sequences U and V, then p divides the product sequence $U * V$. (This group is infinite, of infinite rank, yet has finite torsion.)

The author [**1**, Chapters 4 and 5] generalized this group structure to recurrences of any degree $m \geq 2$, using for division the notion of maximal division. (See also the group constructed for recurrences having a characteristic polynomial with a double root in [**2**].)

The method of Hasse and its direct generalizations have so far only been successful in computing the exact density of maximal prime divisors for some of the few sequences lying in the finite torsion subgroup of the Laxton-Ballot group. The sequence $(1 + F_n)$ is no exception since it is a torsion element of order two.

Indeed, letting $f \in \mathbf{Z}[X]$ have distinct roots $\theta_1, \ldots, \theta_m$ and U be a sequence with characteristic polynomial f, we write, as Ward did [**10**, see (2.4)]

$$U_n = \sum_{i=1}^{m} A_i \frac{\theta_i^n}{f'(\theta_i)}, \quad \forall\, n \in \mathbf{N},$$

where A_i is explicitly representable in terms of $U_0, U_1, \ldots, U_{m-1}$ and the roots of f, see [**1**, Theorem 5.1.6]. The sequence U is fully determined by the m-tuple $\langle A_1, \ldots, A_m \rangle$ and the product $*$ of two sequences having f as characteristic polynomial is defined via component-wise multiplication of the two corresponding m-tuples, see [**1**, pp. 36, 76].

For $m = 3$, we have $A_1 = U_0\theta_2\theta_3 - U_1(\theta_2 + \theta_3) + U_2$ and, letting the permutation (123) act on the subscripts of the θ_i's once and twice, we obtain respectively A_2 and A_3. So one can check the result below

Theorem 8. *Let* $\theta_1 = 1$, $\theta_2 = \varepsilon$, $\theta_3 = \bar{\varepsilon}$ *and* $f(X) = \prod_{i=1}^{3}(X - \theta_i) = (X - 1)(X^2 - X - 1)$. *Then*

$$(1 + F_{n+1}) = \langle -1, 1, 1 \rangle.$$

Note that Theorem 8 implies that $(1 + F_{n+1})$ is torsion of order 2, since $\langle -1, 1, 1 \rangle * \langle -1, 1, 1 \rangle = \langle 1, 1, 1 \rangle$, the identity element of our group. (However, we may say that $(1 + F_n)$ has order two, because the Laxton-Ballot group is actually defined on classes of sequences and two sequences differing from each other by a shift in the subscripts are in the same class. They also share the same maximal divisors. See [**1**, Proposition 5.4.4].

We end Section 5 by a few complementary remarks.

Remarks. (i) Let U be a sequence $\langle A_1, A_2, A_3\rangle$. By Lemma 5.2 of [**10**] (or Theorem 4.4.1 of [**1**]), for essentially all primes p, we have

$$\begin{aligned} &p \text{ is a maximal divisor of } U \text{ at } n \Longleftrightarrow \\ &A_1\theta_1^n \equiv A_2\theta_2^n \equiv A_3\theta_3^n \pmod{(p)}. \end{aligned} \tag{6}$$

Equivalence (6) is a general criterion for maximal division of which Lemma 1 is a particular case.

(ii) Instead of working with the sequence $U_n = 1 + F_n$, we could have used the sequence $V_n = (-1)^{n+1} + F_n$, since $(V_{n-2})_{n\geq 0}$ is the torsion element $\langle -1, 1, 1\rangle$ of the group associated to $g(X) = (X+1)(X^2 - X - 1)$. By (6), we would have obtained for essentially all primes p

$$\begin{aligned} &p \text{ is a maximal divisor of } V \Longleftrightarrow \\ &\exists n \in \mathbf{N} : (-1)^{n+1} \equiv \varepsilon^n \equiv \bar{\varepsilon}^n \pmod{(p)}. \end{aligned} \tag{7}$$

Computing the density of maximal divisors of V using (7), in the manner we used Lemma 1, would have yielded the density of primes for which the pair $(1, -1)$ occurs as consecutive Fibonacci residues modulo p. As we saw in Section 3, this result is equivalent to Theorem 5 of Section 2.

(iii) The computation presented in Section 2 seems to apply well to the general sequence $\langle -1, 1, 1\rangle_f$ for $f(X) = (X \pm 1)(X - \theta)(X - \bar{\theta}) \in \mathbf{Z}[X]$, especially when $\theta/\bar{\theta} = \zeta\theta^k$, where $k \in \mathbf{Z}$ and ζ is a root of 1.

6. Comparison between $P_{\max}(1 + F)$ and $P(L)$. Lagarias [**7**] showed that the set of primes dividing the Lucas numbers (L_n) has density 2/3. But the sequence $L_n = \varepsilon^n + \bar{\varepsilon}^n$ is also of order two in the corresponding Laxton-Ballot group. Moreover, the characteristic polynomial of (L_n), i.e., $X^2 - X - 1$ relates simply to the one of $1 + F$. Thus, our computation and the choice of $(1 + F_n)$ are connected to the article of Lagarias. In fact, it is worthwhile comparing prime divisors of the Lucas numbers to prime maximal divisors of $U = 1 + F$. The prime divisors of (L_n) were studied by Ward [**11**]. And as Ward did, we partition the p's in $\mathcal{P}$ into four classes according to the quadratic characters of 5 and -1 modulo p. Thus, let $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3$ and $\mathcal{P}_4$ be respectively the sets of primes of the forms $20k + 1$ or 9, $20k + 11$ or 19, $29k + 13$ or 17 and $20k + 3$ or 7. Each $\mathcal{P}_i$, $1 \leq i \leq 4$, has density 1/4 by the Dirichlet density theorem.

Note that $\mathcal{P}_3 \cup \mathcal{P}_4 \subset \mathcal{P}_{\max}(1+F_n)$ by Theorem 3 and that $\mathcal{P}_2 \cap \mathcal{P}_{\max}(1+F_n) = \varnothing$ (see the proof of Theorem 4 when $j=1$). For Lucas numbers, we have $\mathcal{P}_2 \cup \mathcal{P}_4 \subset P(L_n)$ and $\mathcal{P}_3 \cap P(L_n) = \varnothing$. These facts were shown by Ward using elementary identities involving the Fibonacci and the Lucas numbers, see [**11**, Lemma 2.2]. They also appear in [**7**] but are presented in the context of Hasse's method.

Now the set of prime divisors of (L_n) in $\mathcal{P}_1$ and the set of maximal prime divisors of $(1+F_n)$ in $\mathcal{P}_1$ both have density $1/6$, by Lemma 3.1 of [**7**] and Theorem 4 of this paper, respectively. Are they the same sets? No. To describe this situation, we need to partition $\mathcal{P}_1$ into three subsets $\mathcal{P}_1^1, \mathcal{P}_1^2, \mathcal{P}_1^3$ respectively according to whether $\mathcal{V}_2(e) \le 1$, $\mathcal{V}_2(e) = 2$ or $\mathcal{V}_2(e) \ge 3$. (Here e is the order of ε modulo Π as defined in Section 2 and $\mathcal{V}_2(e)$ is the 2-adic valuation of e.)

In [**11**, p. 381], Ward showed that, for $p \in \mathcal{P}_1$,

$$p \nmid L \iff \varepsilon^{2q} \equiv \bar{\varepsilon}^{2q} \equiv -1 \pmod{\Pi}, \tag{8}$$

where $p - 1 = 2^j q$ and q is odd. Now the congruence condition in (8) precisely means that $\mathcal{V}_2(e) = 2$ and hence implies that $p|_{\max}(1+F_n)$. Hence, $\mathcal{P}_1^2 \cap P(L) = \varnothing$ and $\mathcal{P}_1^2 \subset P_{\max}(1+F_n)$. But equivalence (8) also implies that $\mathcal{P}_1^1 \cup \mathcal{P}_1^3 \subset P(L)$. And, since $p|_{\max}(1+F_n) \iff 4 \mid e$, we have $\mathcal{P}_1^3 \subset P_{\max}(1+F_n)$ and $\mathcal{P}_1^1 \cap P_{\max}(1+F_n) = \varnothing$. Note that $\delta(\mathcal{P}_1^2) = \delta(\mathcal{P}_1 \backslash P(L)) = 1/4 - 1/6 = 1/12$ and $\delta(\mathcal{P}_1^1) = \delta(\mathcal{P}_1 \backslash P_{\max}(1+F_n)) = 1/4 - 1/6 = 1/12$. Thus, $\delta(\mathcal{P}_1^i) = 1/12$ for all $i \in \{1,2,3\}$.

We summarize the above discussion in a theorem.

Theorem 9. *The synoptic diagram below classifies primes according to whether they divide L or divide $1+F$ maximally, or both divide L and divide $1+F$ maximally. The three subsets $\mathcal{P}_1^i$, $1 \le i \le 3$, of $\mathcal{P}_1$ each have density $1/12$.*

Computational remark. Given a prime p in $\mathcal{P}_1$, finding out which $\mathcal{P}_1^i$ contains p may require a lot of calculation. To decide whether p is in $P(L)$ or not, we can search for the rank of p in (F_n), since we know $p \mid (L_n) \iff r$ is even. But the object of Ward's paper [**11**, Theorem 3.3] was to find better criteria for that purpose. Writing p in $\mathcal{P}_1$ as

	$p \equiv 1 \pmod 4$			$p \equiv 3 \pmod 4$
	$\mathcal{P}_1^1$	$\mathcal{P}_1^2$	$\mathcal{P}_1^3$	$\mathcal{P}_2$
$p \equiv \pm 1 \pmod 5$	L	$1+F$	$L, 1+F$	L
			$\mathcal{P}_3$	$\mathcal{P}_4$
$p \equiv \pm 2 \pmod 5$		$1+F$		$L, 1+F$

$u^2 + 4v^2$, one such criterion stated that if $p \equiv 5 \pmod 8$, then

$$p \mid (L_n) \Longleftrightarrow u \text{ or } v \text{ is } \pm 1 \pmod 5.$$

One point of our remark is that this criterion may also tell whether such a prime divides $(1 + F_n)$ maximally. Indeed, since we necessarily have $5 \mid uv$, if we find that u or $v \equiv \pm 2 \pmod 5$, then $p \nmid (L_n)$, i.e., $p \in \mathcal{P}_1^2$ and $p \mid_{\max} (1 + F_n)$. For instance, $61 \in \mathcal{P}_1$ and is $5 \pmod 8$. But $61 = 5^2 + 4 \cdot 3^2$ and 3 is $-2 \pmod 5$, so $61 \mid_{\max} (1 + F_n)$. Note that the algorithm of Hermite, as improved by Brillhart, see [**4**], efficiently yields the representation of p as $u^2 + 4v^2$.

Finally, let $p \in \mathcal{P}_1$, where $p - 1 = 2^j q$ as above. To determine whether p is, or not, a maximal divisor of $1 + F$, we may compute $l = a^{(p-1)/2^j} \pmod p$, where a is a solution of $X^2 - X - 1 \pmod p$. Indeed, $l = \pm 1 \Longleftrightarrow \mathcal{V}_2(e) \leq 1 \Longleftrightarrow p \nmid_{\max} 1 + F$, i.e., $p \in \mathcal{P}_1^1$. A solution a can be found by solving the congruence $2ta \equiv s + t \pmod p$, where $p = s^2 - 5t^2$, $1 \leq s$, $1 \leq t < \sqrt{4p/5}$, see [**11**, p. 384]. For example, let $p = 29 = L_7$. Then $p = 7^2 - 5 \cdot 2^2 \Longrightarrow s = 7$ and $t = 2$. So $2ta \equiv s + t \Longrightarrow 4a \equiv 9 \pmod p \Longrightarrow (a/p) = 1 \Longrightarrow a^{(p-1)/4} \equiv \pm 1 \pmod p \Longrightarrow 29 \nmid_{\max} (1 + F_n)$.

REFERENCES

1. C. Ballot, *Density of prime divisors of linear recurrences*, Mem. Amer. Math. Soc. **115** (1995).

2. ———, *Group structure and maximal division for cubic recursions with a double root*, Pacific J. Math. **173** (1996), 337–355.

3. D.M. Bressoud, *Factorizations and primality testing*, Springer-Verlag, 1988.

4. J. Brillhart, *Note on representing a prime as a sum of two squares*, Math. Comp. **26** (1972), 1011–1013.

5. J. Brillhart, D.H. Lehmer and J.L. Selfridge, *New primality criteria and factorizations of* $2^m \pm 1$, Math. Comp. **29** (1975), 620–647.

6. H.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. J.C. Lagarias, *The set of primes dividing the Lucas numbers has density* 2/3, Pacific J. Math. **118** (1985), 449–461 and "Errata", **162** (1994), 393–396.

8. R.R. Laxton, *On groups of linear recurrences* I, Duke Math. J. **26** (1969), 721–736.

9. J.P. Serre, *A course in arithmetic*, Springer-Verlag, 1973.

10. M. Ward, *The maximal prime divisors of linear recurrences*, Canad. J. Math. **6** (1954), 455–462.

11. ———, *The prime divisors of Fibonacci numbers*, Pacific J. Math. **11** (1961), 379–386.

Université de Caen, Campus II, Département de Mathématiques, Boulevard du Maréchal Juin, BP 5186, 14032 Caen Cedex, France
E-mail address: ballot@math.unicaen.fr