RANK AND PERIOD OF PRIMES IN THE FIBONACCI SEQUENCE. A TRICHOTOMY

Christian Ballot
Université de Caen, Caen 14032, France
e-mail: ballot@math.unicaen.edu

Michele Elia
Politecnico di Torino, Torino 10129, Italy
e-mail: eliamike@tin.it

(Submitted April 2005-Final Revision July 2005)

ABSTRACT

It has been known since 1985 that one third of the primes do not divide any Lucas number. Here we show that the two remaining thirds can be split naturally into two subsets each of density one third. We prove that the resulting prime trisection can be described in several ways, one of them depending on the value of the ratio of the period T of the Fibonacci sequence $F \pmod p$ to the rank of appearance r of p in F.

1. INTRODUCTION

Consider the sequence $1 + F$ of Fibonacci numbers augmented by 1 and the sequence L of Lucas numbers. Define three sets of primes B_1, B_2 and B_3 as

$$B_1 = \{p;\ p \not| 1 + F\}, \quad B_2 = \{p;\ p \not| L\} \ \text{ and } \ B_3 = \{p;\ p \mid L \text{ and } p \mid 1 + F\}.$$

Here $p \mid L$ (resp. $p \not| L$) means that p divides (resp. does not divide) some Lucas number L_n, whereas $p \mid 1+F$ (resp. $p \not| 1+F$) means that p divides (resp. does not divide) two consecutive terms $1 + F_n$ and $1 + F_{n+1}$ of the sequence $1 + F$.

Results from [**3**] show that the sets B_1, B_2 and B_3 partition the primes and that each B_i has (Dirichlet) density 1/3. Therefore, one may note that this trichotomy refines the known result that the set of primes dividing Lucas numbers has density 2/3; this set is just the union of B_1 and B_3.

Our paper gives two other main characterizations of the sets B_1, B_2 and B_3 (and a couple more as by-products; see Theorem 5.1).

Our second main characterization comes from a result shown in [**12**], namely that the period T of the Fibonacci numbers modulo a prime p and the rank of appearance r of that prime p in the sequence of Fibonacci numbers verify the equation $T = mr$, where the multiplier m can only take three values: 1, 2 or 4. We will prove that $B_1 = \{p;\ T = r\}$, $B_2 = \{p;\ T = 4r\}$ and $B_3 = \{p;\ T = 2r\}$.

The third characterization is shown to be a particular instance of a trichotomy of the primes (observed by Laxton [**9**]) that occurs in relation to any integral quadratic recursion of the type $U_{n+2} = PU_{n+1} - QU_n$ whenever Q is the square of an integer.

This note essentially shows that the three descriptions just mentioned of this prime trichotomy are indeed equivalent.

The paper is divided into five sections. Section 1 is preliminary. Sections 3, 2 and 4 correspond respectively to the three descriptions aforementioned of our prime trichotomy.

Section 2 is very short and reproves in a different manner results from [**12**].

Since it is known [**12**] that for any $k \neq 1$ or 9, the value of m is a function of the residue class k of p modulo 20, Section 3 also contains a lengthy, yet non exhaustive, computational remark (Remark 3.5) giving some efficient tests for deciding on the value of m when dealing with a prime p of the form $20n+1$ or $20n+9$. Some such tests based on the representation of p as u^2+4v^2 were derived by Ward [**13**]. Here we add some new tests based on the representation of p as $a^2 + ab - b^2$.

Section 5 is conclusive. The main results are summarized in Theorem 5.1. And a whole family of recursions, for which Theorem 5.1 fully generalizes, is pointed out.

2. PRELIMINARIES

The n-th Fibonacci number will be denoted by the letter F_n. Hence $F_0 = 0$, $F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 0$. We have $F_n = (\epsilon^n - \bar{\epsilon}^n)/(\epsilon - \bar{\epsilon})$, where ϵ and $\bar{\epsilon}$ are the two real roots of $X^2 - X - 1 \in \mathbb{R}[X]$. The letter σ will represent the non-trivial automorphism of the Galois group of $\mathbb{Q}(\sqrt{5}\,)$ over $\mathbb{Q}$. We will call "conjugation" the action of applying σ to some identity. Putting $\epsilon = (1 + \sqrt{5})/2$, we have $\bar{\epsilon} = \sigma(\epsilon)$. Thus $\mathbb{Z}[\epsilon]$ is the ring of algebraic integers of $\mathbb{Q}(\sqrt{5}\,)$. For p a rational prime, (p) denotes the ideal generated by p in $\mathbb{Z}[\epsilon]$. The Lucas numbers L_n form the companion Lucas sequence to the Fibonacci sequence and they are defined by $L_n = \epsilon^n + \bar{\epsilon}^n$ for any $n \geq 0$.

The 2-adic valuation of a rational integer a is written $\mathcal{V}_2(a)$ and the fact that two integers a and b have the same 2-adic valuation will often be written $a \sim b$. Thus, $\mathcal{V}_2(8) = 3$, $2 \sim 6$ and $7 \sim 1$.

The Legendre symbol $(mod\ p)$ will be written $(* \mid p)$.

Definition 1.1: (Period T) Let p be a rational prime. The period T of the Fibonacci sequence $(mod\ p)$ is the least integer $m > 0$ such that $F_{n+m} \equiv F_n\ (mod\ p)$ for all $n \geq 0$.

Proposition 1.2: *For any prime p, the period T equals the order of ϵ $(mod\ (p))$ in $\mathbb{Z}[\epsilon]$.*

Proof: Because the characteristic polynomial $X^2 - X - 1$ has a constant term -1 not divisible by p, the Fibonacci sequence $(mod\ p)$ obeys a recursion of minimal order 2 for any p and the period T is the least integer $n > 0$ such that

$$F_n \equiv 0\ (mod\ p) \quad \text{and} \quad F_{n+1} \equiv 1\ (mod\ p).$$

An easy induction yields the classical identity $\epsilon^{n+1} = \epsilon F_{n+1} + F_n$, from which we immediately get the equivalence

$$\begin{cases} F_n \equiv 0 \\ F_{n+1} \equiv 1 \end{cases} (mod\ p) \quad \Longleftrightarrow \quad \epsilon^n \equiv 1\ (mod\ (p)).$$

(For $\Longleftarrow$) use the fact that $(1, \epsilon)$ is an integral basis of $\mathbb{Z}[\epsilon]$ so that $\epsilon F_{n+1} + F_n \equiv \epsilon\ (mod\ (p)) \implies p \mid F_{n+1} - 1$ and $p \mid F_n$.) $\square$

Definition 1.3: (Rank r) The rank $r = r(p)$ of a prime p in the Fibonacci sequence is the least integer $m > 0$ such that F_m is divisible by p.

Proposition 1.4: *For any prime p, the rank r equals the order of $-\epsilon^2$ $(mod\ (p))$ in $\mathbb{Z}[\epsilon]$.*

Properties of the rank: For any p, the rank is also the least integer $r > 0$ such that $\epsilon^r \equiv \bar{\epsilon}^r\ (mod\ (p))$. Since $\epsilon/\bar{\epsilon} = -\epsilon^2$, we see that Proposition 1.4 holds. We also recall here

that r is even if and only if $p \mid L_n$ for some n. For split primes, i.e. primes $p \equiv \pm 1 \ (mod\ 5)$, $r \mid p-1$, whereas for inert primes $\equiv \pm 2 \ (mod\ 5)$, $r \mid p+1$. We also recall the generalized Euler criterion that states that $r \mid (p-\eta_p)/2 \iff (-1 \mid p) = 1$, where η_p is the Legendre symbol $(5 \mid p)$ (See Prop. 7 and the references given in its proof in [**3**]).

3. A TRICHOTOMY OF THE SET OF PRIMES BASED ON COMPARING T AND r

Theorem 2.1: *For any odd prime p, the period T of the Fibonacci sequence $F_n \ (mod\ (p))$ and the rank r of p in (F_n) satisfy*

(1) T is even, (2) $r \mid T$, and (3) $T \mid 4r$.

We have, as an immediate consequence, that $T = r,\ 2r$ or $4r$.

Proof: (1) By Prop. 1.2, we have $\epsilon^T \equiv 1 \ (mod\ (p))$. Conjugation yields $\bar{\epsilon}^T \equiv 1 \ (mod\ (p))$. Hence since $\epsilon\bar{\epsilon} = -1$ we have $1 \equiv \epsilon^T\bar{\epsilon}^T = (-1)^T \ (mod\ (p))$, which implies that T is even.

(2) Since T is even, $\epsilon^T \equiv 1 \ (mod\ (p)) \Longrightarrow (-\epsilon^2)^T \equiv 1 \ (mod\ (p))$. Hence $r \mid T$.

(3) $(-\epsilon^2)^r \equiv 1 \Longrightarrow \epsilon^{2r} \equiv (-1)^r \implies \epsilon^{4r} \equiv 1 \ (mod\ (p))$. Hence $T \mid 4r$. □

Lemma 2.2: *Let p be an odd prime. Then $T = 4r \iff r$ is odd.*

Proof: Use the proof of point (3) of Theorem 2.1. Indeed if r is odd, then $\epsilon^{2r} \equiv (-1)^r = -1$ so that $T \not\mid 2r$. Hence by Theorem 2.1, $T = 4r$. Conversely $T = 4r \Longrightarrow \epsilon^{2r} \not\equiv 1$, i.e. $(-1)^r \not\equiv 1 \ (mod\ (p))$, which implies that r is odd. □

Lemma 2.3: *For any prime p, if $4 \mid T$, then $T = 2r$ or $T = 4r$.*

Proof: Indeed $(-\epsilon^2)^{T/2} \equiv (-1)^{T/2}\epsilon^T \equiv 1 \times 1 \equiv 1 \ (mod\ (p)) \implies r \mid T/2 \Longrightarrow T = 2r$ or $T = 4r$. (In particular using Theorem 2.1 and Lemma 2.2, $4 \mid r \Longrightarrow T = 2r$.) □

Lemma 2.4: *For primes $p \equiv \pm 2 \ (mod\ 5)$, we have $T \sim 2(p+1)$.*

Proof: For inert primes p the Frobenius automorphism $Frob[(p)|p]$ is the non-trivial automorphism σ. Therefore $\epsilon^{p+1} = \epsilon^p\epsilon \equiv \sigma(\epsilon)\epsilon = \bar{\epsilon}\epsilon = -1 \ (mod\ (p))$, so $T \mid 2(p+1)$ and $T \not\mid p+1$. Hence, $T \sim 2(p+1)$. □

4. EQUIDISTRIBUTION OF THIS PRIME TRICHOTOMY

To any monic polynomial $f \in \mathbb{Z}[X]$ of degree $m \geq 2$, with $f(0) \neq 0$ and at most one double root, is associated a group structure in which the group operation preserves *maximal division* for any prime p. The group elements are classes of integral linear recurring sequences with minimal characteristic polynomial f. If $Disc\ f \neq 0$, two such sequences are in the same class provided they differ from each other by a rational scalar and/or by a shift of indices. We refer the reader interested in this group to [**9**] for the case $m = 2$, [**1**] for $m \geq 2$ and $Disc\ f \neq 0$, [**2**] for f having one double root and [**5**] (p. 4 and 106-7) for a concise summary. Let $U = (u_n)_{n\geq 0}$ be an integral linear recurring sequence whose minimal characteristic polynomial is f. Then a prime p is said to divide U if there are $m-1$ consecutive terms of U that are divisible by p. This type of division is called "maximal division", and for quadratic recursions it simply means that some term u_n is divisible by p. This infinite abelian group has a finite torsion subgroup and for the few rare sequences that are 'torsion' it is generally possible to compute the exact density of the set of primes that divide them. The method to use is an adaptation of the method achieved by Hasse [**6**] for sequences of the type $a^n + 1$, where $a \in \mathbb{Z}$; it is unconditional in the sense that it does not depend on generalized Riemann hypotheses.

The prime density of a set S of rational primes we refer to is the Dirichlet density, defined (if it exists) as

$$\lim_{s\to 1^+} \frac{\sum_{p\in S} p^{-s}}{\sum_p p^{-s}} = \delta(S).$$

The sequence L of Lucas numbers, defined by $L_n = \epsilon^n + \bar{\epsilon}^n$, and the sequence $1+F$ of Fibonacci numbers augmented by 1, are the only order 2 sequences in the groups associated to (respectively) $X^2 - X - 1$ and $(X-1)(X^2 - X - 1)$. Both the prime divisors of L and the prime divisors of $1+F$ have Dirichlet density equal to $2/3$ (see resp. [**8**] and [**3**]).

It then seemed natural to compare these two sets of primes. So in [**3**], we presented the diagram below in which the sequence L or $1+F$ appears if and only if the corresponding primes divide it

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

This diagram is conspicuous for showing that *any* prime not 2 or 5 belongs to exactly one of the three sets

$$B_1 = \{p;\ p \mid L \text{ and } p \not\mid 1+F\}, \quad B_2 = \{p;\ p \not\mid L \text{ and } p \mid 1+F\}, \text{ or}$$
$$B_3 = \{p;\ p \mid L \text{ and } p \mid 1+F\}. \tag{1}$$

Note that, since any p not dividing L divides $1+F$, we may define B_2 more simply as $\{p;\ p \not\mid L\}$. Similarly we may define B_1 as $\{p;\ p \not\mid 1+F\}$. Here $\mathcal{P}_1$, $\mathcal{P}_2$, $\mathcal{P}_3$ and $\mathcal{P}_4$ are respectively the sets of primes of the forms $20k+1$ or 9, $20k+11$ or 19, $20k+13$ or 17 and $20k+3$ or 7. Each $\mathcal{P}_i$, $1 \le i \le 4$, has density $1/4$ by the Dirichlet density theorem.

The three subsets $\mathcal{P}_1^1$, $\mathcal{P}_1^2$, $\mathcal{P}_1^3$ of $\mathcal{P}_1$ were respectively defined according as $\mathcal{V}_2(e) \le 1$, $\mathcal{V}_2(e) = 2$ or $\mathcal{V}_2(e) \ge 3$. (The letter e denoted the order of ϵ modulo Π where Π was a fixed prime ideal lying over p in $\mathbb{Z}[\epsilon]$.) These three subsets were shown to each have a Dirichlet density equal to $1/12$. So each B_i, $i = 1, 2, 3$ has a density equal to $1/4 + 1/12 = 1/3$.

Hence, an equidistributed trichotomy of the set of primes was observed. We propose to characterize the classes B_1, B_2 and B_3 in two alternative ways that may be more evocative or more natural, one of them being the prime trichotomy of Section 1.

Theorem 3.1: *Let T and r denote the period and rank associated to a prime p and the Fibonacci sequence. Then the three sets B_1, B_2 and B_3 defined in (1) have the alternative characterizations*

$$B_1 = \{p;\ \mathcal{V}_2(T) = 1\} = \{p;\ T = r\},$$
$$B_2 = \{p;\ \mathcal{V}_2(T) = 2\} = \{p;\ T = 4r\},$$
$$\textit{and} \quad B_3 = \{p;\ \mathcal{V}_2(T) \ge 3\} = \{p;\ T = 2r\}.$$

We first gather in one lemma two results shown in [**3**], Section 2.

Lemma 3.2: *Let p be a prime not 2 or 5 and Π a prime ideal in $\mathbb{Z}[\epsilon]$ above p. Then*

$$p \text{ divides } 1+F \iff \exists n \in \mathbb{N} \,:\, -1 \equiv \epsilon^n \equiv \bar{\epsilon}^n \,(mod\,(p)) \iff 4 \mid e,$$

where e is the order of ϵ $(mod\,\Pi)$.

Remark 3.3: For split primes p in $\mathbb{Z}[\epsilon]$ for which $(p) = \Pi\,\bar{\Pi}$, let $\bar{e}$ denote the order of ϵ $(mod\ \bar{\Pi})$. Then multiplying the congruence $\epsilon^e \equiv 1\ (mod\ \Pi)$ by $\bar{\epsilon}^e$ and conjugating yields $(-1)^e \equiv \epsilon^e\ (mod\,\bar{\Pi})$. Therefore

$$\bar{e} \text{ divides } \begin{cases} e & , \text{ if } e \text{ is even,} \\ 2e & , \text{ if } e \text{ is odd.} \end{cases}$$

But the roles of e and $\bar{e}$ can be permuted so that either $e = \bar{e}$, if both e and $\bar{e}$ are even, or $e = 2\bar{e}$, or $\bar{e} = 2e$ if $\bar{e}$, resp. e, is odd. But T being the order of ϵ $(mod\ (p))$ is the least common multiple of e and $\bar{e}$, so that $T = e$ if e is even, or $T = 2e$ if e is odd. Hence, $4 \mid e \iff 4 \mid T$. So we may replace e by T in Lemma 3.2.

Proof of Theorem 3.1: Because B_1, B_2 and B_3 partition the set of primes it is sufficient to show the three implications below

i) $p \in B_1 \implies \mathcal{V}_2(T) = 1$ and $T = r$,
ii) $p \in B_2 \implies \mathcal{V}_2(T) = 2$ and $T = 4r$,
iii) $p \in B_3 \implies \mathcal{V}_2(T) \geq 3$ and $T = 2r$.

For (i), $p \mid L \implies r$ is even, and $p \nmid 1+F \implies 4 \nmid T$, where the second implication comes from Lemma 3.2 and Remark 3.3. Now $2 \mid r$ and $4 \nmid T$ together with the knowledge that $T = r,\ 2r$ or $4r$ imply $T = r$. Also, T is even and $4 \nmid T \implies T \sim 2$, that is $\mathcal{V}_2(T) = 1$.

For (ii), $p \nmid L \implies r$ is odd, so that by Lemma 2.2, $T = 4r$. Therefore, $\mathcal{V}_2(T) = 2$.

For (iii), if $p \in \mathcal{P}_4$, i.e. $p \equiv 3\ (mod\ 4)$ and $p \equiv \pm 2\ (mod\ 5)$ then $T \sim 2(p+1) \implies \mathcal{V}_2(T) \geq 3$. If on the contrary $p \in \mathcal{P}_1^3$ then by definition $\mathcal{V}_2(e) \geq 3$, so that $\mathcal{V}_2(T) \geq 3$. Now $p \mid 1+F \implies \exists n > 0$ such that $-1 \equiv \epsilon^n \equiv \bar{\epsilon}^n\ (mod\ (p))$. Since T is the order of $\epsilon\ (mod\ (p))$, we have $T \mid 2n$ and $T \nmid n$. Therefore $T \sim 2n$. But $r \mid n$ so $T = 2r$ or $T = 4r$. Since $p \mid L$, r is even and so $T \neq 4r$. Hence $T = 2r$. □

Remark 3.4: Another immediate characterization of our trichotomy based on the power of 2 dividing r emerges from Theorem 3.1, namely $B_1 = \{p;\ \mathcal{V}_2(r) = 1\}$, $B_2 = \{p;\ \mathcal{V}_2(r) = 0\}$ and $B_3 = \{p;\ \mathcal{V}_2(r) \geq 2\}$.

Remark 3.5: a) Note that, by Euler's generalized criterion, primes $p \equiv 5\ (mod\ 8)$ and $\pm 1\ (mod\ 5)$ verify $r \mid (p-1)/2$ so that $\mathcal{V}_2(r) \leq 1$. Therefore, they are either in B_1 or B_2. Hence, deciding whether p is in B_1 or B_2 amounts to deciding whether p divides L or not. Ward [**13**] used the representation of p as $u^2 + 4v^2$ and showed that $p \in B_1 \iff u$ or $v \equiv \pm 1\ (mod\ 5)$. Alternatively, one may use the representation of p as $a^2 + ab - b^2$. Indeed, putting $\Pi = (a + b\epsilon)$ (and $\bar{\Pi} = (a + b\bar{\epsilon})$), we have $p \in B_1 \iff T \sim 2 \iff \epsilon^{(p-1)/2} \equiv 1\ (mod\ \Pi)$, taking Remark 3.3 into account. But the latter statement is equivalent to asserting that the generalized Legendre symbol $(\epsilon \mid \Pi) = 1$. And $(\epsilon \mid \Pi) = (b^2\epsilon \mid \Pi) = (a + b\epsilon - a \mid \Pi)(b \mid \Pi) = (-ab \mid \Pi) = (-ab \mid p) = (ab \mid p)$. Therefore $p \in B_1 \iff (ab \mid p) = 1$.

b) For a prime p in $\mathcal{P}_1$ such that $\mathcal{V}_2(p-1) = j \geq 3$, one may also efficiently decide on which B_i, $i = 1, 2$ or 3 contains p. Compute the reduced residue l of $\alpha^{(p-1)/2^{j-1}}\ (mod\ p)$, where α is a root of $X^2 - X - 1\ (mod\ p)$. Then $l = 1 \implies \mathcal{V}_2(T) = 1 \implies p \in B_1$. If $l \equiv -1\ (mod\ p)$, then $\mathcal{V}_2(T) = 2$ and $p \in B_2$. If $l \not\equiv \pm 1\ (mod\ p)$, then $p \in B_3$. Finding α can

be done in various ways. Either use Ward's suggestion (see [**13**], (4.6) and (4.7)), or compute $\sqrt{5}$ $(mod\ p)$ using the $O(\log p)$ algorithm of Lehmer [**10**]. Then $\alpha = 2^{-1}(1+\sqrt{5})$ $(mod\ p)$.

Alternatively find a representation of p as a^2+ab-b^2 (an efficient algorithm generalizing [**4**] for finding such a and b can be found in [**7**] or [**14**]). Then depending on whether the generalized Legendre symbol $(\epsilon \mid \Pi)_{2^{j-1}} = \epsilon^{(p-1)/2^{j-1}}$ $(mod\ \Pi)$, where again $\Pi = (a+b\epsilon)$, is 1, -1 or is not ± 1, we have resp. $p \in B_1$, $p \in B_2$ or $p \in B_3$. And this symbol can be evaluated as a Legendre symbol over the rationals. Indeed, $(\epsilon \mid \Pi)_{2^{j-1}}$ is equal to

$$(b^{2^{j-1}}\epsilon \mid \Pi)_{2^{j-1}} = (b^{2^{j-1}-1}(a+b\epsilon-a) \mid \Pi)_{2^{j-1}} = (-ab^{2^{j-1}-1} \mid \Pi)_{2^{j-1}} = (ab^{2^{j-1}-1} \mid p)_{2^{j-1}}.$$

Remark 3.6: The identity sequence of the group associated to $(X-1)(X-\epsilon)(X-\bar{\epsilon})$ is the sequence I with $I_0 = I_1 = 0$ and $I_2 = 1$. One defines the *rank of maximal division* $r_{max}(p)$ of a prime p as the least $m > 0$ such that $p \mid I_m$ and $p \mid I_{m+1}$. It is interesting to note that the period T of F_n $(mod\ p)$ is also the rank $r_{max}(p)$, as can be easily verified using the theory developed in Chap. 3 of [**1**].

5. A THIRD PRIME TRICHOTOMY STUDIED BY LAXTON

Let $f(X) = X^2 - PX + Q \in \mathbb{Z}[X]$, $Q \neq 0$, with roots α and β. Laxton [**9**] had shown that if Q is not a square then the only 'torsion' sequence of order 2 in the group associated to f – the group we mentioned early in Section 3 – is the companion Lucas sequence $V_n = \alpha^n + \beta^n$. But he also showed that if $Q = R^2$, $R \in \mathbb{Z}$ then, besides V, there are two more order 2 sequences, namely $A_n = U_{n+1} + RU_n$ and $B_n = U_{n+1} - RU_n$. Here $U_n = (\alpha^n - \beta^n)/(\alpha - \beta)$ is the Lucas sequence associated to f. Moreover, the two sequences A and B have no prime divisors in common and none in common with V. Indeed $A_nB_n = U_{n+1}^2 - QU_n^2 = U_{2n+1}$ so only primes of odd rank may divide A or B. If a prime p divided both A and B it would divide the sequence V since $V = A * B$ where $*$ is the group operation (we have a copy of the Klein group and the group operation $*$ preserves division by primes). Therefore to each such f is associated another prime trichotomy which was – at least on an experimental basis – observed to be equidistributed for many such f's.

By Remark 3.4, B_3 is the set of primes whose rank r is divisible by 4. But these primes are the primes dividing L_{2n}. Indeed, let p be an odd prime. Since $F_{4n} = L_{2n}F_{2n}$ and $L_{2n}^2 - 5F_{2n}^2 = 4$, if p divides L_{2n}, then $p \mid F_{4n}$ and $p \nmid F_{2n}$. So $r \mid 4n$ and $r \nmid 2n$, which implies $4 \mid r$. The converse goes similarly. Now $L_{2n} = \epsilon^{2n} + \bar{\epsilon}^{2n}$ is the V-sequence associated with $f(X) = X^2 - 3X + 1 = X^2 - (\epsilon^2 + \bar{\epsilon}^2)X + (\epsilon\bar{\epsilon})^2$, whereas the U-sequence is F_{2n}. Since $Q = 1 = 1^2$ the two other 'torsion' sequences of order 2 are $A_n = F_{2(n+1)} + F_{2n} = L_{2n+1}$ and $B_n = F_{2(n+1)} - F_{2n} = F_{2n+1}$. The primes dividing A and B are thus easily seen to be (resp.) the primes of rank r with $\mathcal{V}_2(r) = 1$ and the primes of rank r with $\mathcal{V}_2(r) = 0$. And we have shown that our trichotomy is the one associated to the Klein subgroup of the group associated to $X^2 - 3X + 1$.

6. SUMMARY AND CONCLUDING REMARKS

First we summarize the foregoing discussion in a theorem.

Theorem 5.1: *The set of primes p not 2 or 5 is partitioned into three disjoint subsets B_1, B_2 and B_3 that can be described in one of five alternative ways as*

$$\begin{aligned} B_1 &= \{p;\ p \mid L \text{ and } p \not\mid 1+F\} \\ &= \{p;\ \mathcal{V}_2(T)=1\} = \{p;\ T=r\} \\ &= \{p;\ \mathcal{V}_2(r)=1\} = \{p;\ p \mid (L_{2n+1})\}, \\ B_2 &= \{p;\ p \not\mid L\} \\ &= \{p;\ \mathcal{V}_2(T)=2\} = \{p;\ T=4r\} \\ &= \{p;\ \mathcal{V}_2(r)=0\} = \{p;\ p \mid (F_{2n+1})\}, \\ \text{and}\quad B_3 &= \{p;\ p \mid L \text{ and } p \mid 1+F\} \\ &= \{p;\ \mathcal{V}_2(T)\geq 3\} = \{p;\ T=2r\} \\ &= \{p;\ \mathcal{V}_2(r)\geq 2\} = \{p;\ p \mid (L_{2n})\}. \end{aligned}$$

Each B_i, $i=1,2$ and 3, has Dirichlet density $1/3$.

Depending on the point of view chosen to describe, or acknowledge this prime trichotomy, one may, or may not, be able to say that it generalizes to other recursions. But every aspect of the prime trichotomy associated to the Fibonacci recursion that we have studied at least carries over to a large family of recursions. Indeed, let d be a squarefree integer ≥ 3 and $\epsilon = a+b\sqrt{d}$ be the fundamental unit of the ring of integers of $\mathbb{Q}(\sqrt{d}\,)$. Assume ϵ has norm -1. Then, for odd primes not dividing d, Theorem 5.1 remains entirely true if F is replaced by U, where $U_n = (\epsilon^n - \bar{\epsilon}^n)/(\epsilon - \bar{\epsilon})$, T is the period of U_n $(mod\ p)$ and r the rank of appearance of p in U. Of course L is replaced by V, where $V_n = \epsilon^n + \bar{\epsilon}^n$ and $1+F$ is replaced by the only order 2 'torsion' sequence of the group associated to $(X-1)(X^2-2aX-1)$. This sequence K has, according to Remark 4.6.2 of [**1**], initial values $2, 2, 2+2a$. It turns out to be $K_n = 1+U_n+U_{n-1}$. (The sequences A and B described in Section 4 are resp. $A_n = V_{2n+1}$ and $B_n = 2aU_{2n+1}$.) That B_2 still has Dirichlet density $1/3$ can be easily checked by reading the proof of the Theorem shown in [**11**] in the -1 norm case with $d \neq 2$. That the disjoint union $B_2 \cup B_3$ has density $2/3$ can be done by a straight adaptation of the two lemmas and the two theorems of [**3**], Section 2, to yield the density of primes dividing two consecutive terms of K, since K replaces $1+F$.

REFERENCES

[1] C. Ballot. "Density of Prime Divisors of Linear Recurrences." *Mem. Am. Math. Soc.* **551** (1995): 102 .

[2] C. Ballot,. "Group Structure and Maximal Division for Cubic Recursions with a Double Root." *Pacific J. Math.* **173.2** (1996): 337-355.

[3] C. Ballot. "The Density of Primes p, Such that -1 is a Residue Modulo p of Two Consecutive Fibonacci Numbers, is 2/3." *Rocky Mt. J. Math.* **3** (1999): 749-761.

[4] J. Brillhart. "Note on Representing a Prime as a Sum of Two Squares." *Math. Comp.* **29** (1972): 1011-1013.

[5] G. Everest et als. *Recurrence Sequences*, Mathematical surveys and monographs, vol. 104, AMS (2003).
[6] H. H. Hasse. "Uber 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.
[7] K. Hardy, J. Muskat, K. Williams. "Solving $n = au^2 + buv + cv^2$ using the Euclidean Algorithm." *Util. Math.* **38** (1990): 225-236.
[8] J. C. Lagarias. "The Set of Primes Dividing the Lucas Numbers has Density 2/3." *Pacific J. Math.* **118.2** (1985): 449-461 and "Errata" **162** (1994): 393-396.
[9] R. R. Laxton. "On Groups of Linear Recurrences I." *Duke Math. J.* **26** (1969): 721-736.
[10] D. H. Lehmer. "Computer Technology Applied to the Theory of Numbers." *MAA Studies in Mathematics* **6** (1969): 117-151.
[11] P. Moree & P. Stevenhagen. "Prime Divisors of Lucas Sequences." *Acta Arithm.* **82.4** (1997): 403-410.
[12] J. Vinson. "The Relation of the Period Modulo to the Rank of Apparition of m in the Fibonacci Sequence." *Fib. Quart.* **1.2** (1963): 37-45.
[13] M. Ward. "The Prime Divisors of Fibonacci Numbers." *Pacific J. Math.* **11** (1961): 379-386.
[14] K. Williams. *Some Refinements of an Algorithm of Brillhart*, Dilcher, Karl (ed.), Number theory. Fourth conference of the Canadian Number Theory Association, July 2-8, 1994, RI: American Mathematical Society. CMS Conf. Proc. 15, (1995) 409-416.

AMS Classification Numbers: 11B37, 11B39, 11B83, 11R45

✠ ✠ ✠