FIBONACCI FIELDS

T. MacHenry
Department of Mathematics and Statistics
York University, 4700 Keele St., Toronto, Ontario, Canada M3J 1P3
(*Submitted March 1998-Final Revision July 1998*)

0. INTRODUCTION

In this paper, we consider fields determined by the n^{th} roots of the zeros α and β of the polynomial x^2-x-1; α is the positive zero. The tools for studying these fields will include the Fibonacci and Lucas polynomials. Generalized versions of Fibonacci and Lucas polynomials have been studied in [1], [2], [3], [4], [5], [6], [7], and [12], among others. For the most part, these generalizations consist of considering roots of more general quadratic equations that also satisfy Binet identities. However, it is just the simplest version of these polynomials that we shall need for the results in this paper. (For a far-reaching generalization of all of these generalizations in the context of multiplicative arithmetic functions, see [9].) These polynomials determine many of the properties of the root fields; e.g., they provide the defining polynomials for those fields; they yield a collection of algebraic integers which behave like the Fibonacci numbers and the Lucas numbers in the ring of rational integers; they determine the discriminants of these fields; and, they provide a means of embedding which gives the lattice structure of the fields.

In Part 1, we list properties of these polynomials which we shall need later.

In Part 2, the (odd) m^{th} roots of α and β are discussed; the constant a_m which is, essentially, the sum of two conjugate roots, is introduced. One of two important theorems here is Theorem 2.1, which tells us that the m^{th} Lucas polynomial evaluated at a_m is, up to sign, equal to 1. This will enable us to define a new set of polynomials (by adding a constant to the Lucas polynomial) which, in Part 4, will turn out to be irreducible over the rationals and, hence, will provide us with some useful extension fields (Theorem 4.2). The other important theorem in Part 2 is Theorem 2.2, which tells us that the m^{th} Lucas polynomial evaluated at a_{mn} is a_n. This theorem will lead to an embedding theorem for our fields in Part 4 (Lemma 4.2.2).

In Part 3, we introduce numbers in our extension fields generalizing the Fibonacci numbers, which are algebraic integers in these fields and which turn out to have a peculiar quasi-periodic behavior (Theorem 3.4). (In a sequel to [9], this behavior will be seen to be one typically associated with arithmetic functions.)

In Part 4, the lattice structure of this family of fields is investigated (Lemma 4.2.2, Corollary 4.2.3, Theorem 4.3). Theorem 4.4 tells us that it is the Fibonacci polynomials which provide us with the discriminants of our fields.

The remainder of the paper is occupied with some calculations using a well-known matrix representation of the fields, illustrating computations which produce units and primes in these fields.

The author is indebted to the referee for many helpful suggestions for which he is grateful; especially, he would like to thank the referee for calling to his attention the rich theory of quadratic fields of *Richaud-Degert* type and of R. A. Mollin's book [10]. The fields studied here are extensions of a field of this type.

1. THE POLYNOMIALS $U_n(t)$ AND $V_n(t)$

Here we list some of the well-known properties of the Fibonacci and Lucas polynomials, $U_n(t)$ and $V_n(t)$, that we shall need to use in this paper (see, e.g., [3] and [4]). In [3], [2], and [5], these polynomials were defined explicitly by formulas equivalent to

$$U_m(t) = \sum_{k=0}^{\infty} P_k(m) t^{m-2k-1}, \quad P_k(m) = \binom{m-k-1}{k}, \; k \le \frac{m}{2}, \tag{1.1}$$

$$V_m(t) = \sum_{k=0}^{\infty} \frac{m}{m-2k} P_k(m) t^{m-2k} + \varepsilon_m, \quad \varepsilon_m = \begin{cases} 0, & m \text{ odd}, \\ 2, & m \text{ even}. \end{cases} \tag{1.2}$$

$U_0(t) = 0$, $U_1(t) = 1$, $V_0(t) = 2$, $V_1(t) = t$.

Equivalently, we could have defined $U_n(t)$ and $V_n(t)$ by letting $A(t)$ and $B(t)$ be the roots of the polynomial $p(x) = x^2 - tx - 1$, and setting

$$U_n(t) = \frac{A^n(t) - B^n(t)}{A(t) - B(t)}, \tag{1.3}$$

$$V_n(t) = A^n(t) + B^n(t), \tag{1.4}$$

i.e., the well-known Binet formulas (e.g., see [3] or [6]). From these formulas, it is easy to see that the recursion relation

$$Y_{n+1}(t) = tY_n(t) + Y_{n-1}(t) \tag{1.5}$$

is satisfied by the Fibonacci and Lucas polynomials* [3]. In fact, theses identities provide a painless path for finding most of the identities involving the two sequences of polynomials. Such an identity, which we shall need below, is

$$V_m(V_n(t)) = V_{mn}(t), \quad ([3], 6.2(\text{i})). \tag{1.6}$$

It is, however, equally easy to use the recursion (2.5) to prove that

$$d/dt(V_n(t)) = nU_n(t), \quad ([4], (2.4)), \tag{1.7}$$

which, in turn, gives a short proof using (2.6) of the fact (well known) that U_k divides U_{ks}, with the additional feature of displaying the factors explicitly. To wit:

$$d/dt[V_m(V_n(t))] = mnU_n(t)U_m(V_n(t)) = d/dt[V_{mn}(t)] = mnU_{mn}(t).$$

Thus, the other factor is $U_m(V_n(t))$.

2. THE NUMBERS γ_m, δ_m, a_m

Define γ_m and δ_m up to roots of unity by

$$\gamma_m^m = \alpha, \quad \delta_m^m = \beta.$$

---

* The first six polynomials in these two sequences are:

$U_0(t) = 0$	$U_2(t) = t$	$U_4(t) = t^3 + 2t$	$V_2(t) = t^2 a = 2$	$V_0(t) = 2$	$V_4(t) = t^4 + 4t^2 + 2$
$U_1(t) = 1$	$U_3(t) = t^2 + 1$	$U_5(t) = t^4 + 3t^2 + 1$	$V_1(t) = t$	$V_3(t) = t^3 + 3t$	$V_5(t) = t^5 + 5t^3 + 5t$

Since $(\gamma_m\delta_m)^m = \alpha\beta = -1$, we have that $\boxed{\gamma_m\delta_m = \omega_m,}$ where ω_m is a primitive 2^m-th root of unity. When m is odd, then at least one of the γ_m and δ_m is real. Define a_m by $\boxed{\gamma_m + \delta_m = a_m\omega_m^2.}$ Note that $a_1 = 1$. Clearly, $\gamma_1 = \alpha = A(a_1)$ and $\delta_1 = \beta = B(a_1)$. It follows that

$$\gamma_m = \frac{1}{2}(a_m + (a_m^2 + 4)^{1/2})\omega_m^{(m+1)/2} = A(a_m\omega_m^{(m+1)/2}),$$
$$\delta_m = \frac{1}{2}(a_m - (a_m^2 + 4)^{1/2})\omega_m^{(m+1)/2} = B(a_m\omega_m^{(m+1)/2})$$

and

$$A(a_m\omega_m^{(m+1)/2}) = \omega_m^{(m+1)/2}A(a_m), \quad B(a_m\omega_m^{(m+1)/2}) = \omega_m^{(m+1)/2}B(a_m).$$

So

$$\boxed{\begin{aligned}\gamma_m &= \omega_m^{(m+1)/2}(a_m),\\ \delta_m &= \omega_m^{(m+1)/2}(a_m).\end{aligned}}$$

Thus,

$$\begin{aligned}A^m(a_m\omega_m^{(m+1)/2}) + B^m(a_m\omega_m^{(m+1)/2}) &= (-1)^{(m+1)/2}(A^m(a_m) + B^m(a_m))\\ &= V_m(a_m) = \gamma_m^m + \delta_m^m = \alpha + \beta = 1,\end{aligned}$$

and so

Theorem 2.1: $(-1)^{(m+1)/2}V_m(a_m) - 1 = 0$, m odd. □

Hence, a_m is a root of the polynomial $D_m(t) = V_m(t) - (-1)^{(m+1)/2}$.

Proposition 2.1.1: $\alpha = \frac{1}{2}(1 + R(a_m))U_m(a_m), \ \beta = \frac{1}{2}(1 - R(a_m))U_m(a_m), \ R(t) = (t^2 + 4)^{1/2}$,

is implied by the next proposition.

Proposition 2.1.2: $A^m(a_m) = \alpha, \ B^m(a_m) = \beta$.

Proposition 2.1.3: $A^m(a_{mn}) = \gamma_n, \ B^m(a_{mn}) = \delta_n$.

Proof: $A^{mn}(a_{mn}) = \alpha_n^n = \gamma_n^n$.

In particular,

Theorem 2.2: $V_m(a_{mn}) = a_n$, up to the roots of unity.

Proof: $A^{mn}(a_{mn}) + B^{mn}(a_{mn}) = V_m(a_{mn}) = \gamma_n + \delta_n = a_n$ (up to roots of unity).

3. GENERALIZED FIBONACCI AND LUCAS NUMBERS

The algebraic numbers $U_k(a_m)$ can be thought of as a generalization of the Fibonacci numbers. However, we need an unambiguous notation for them, so remembering that m is odd in this paper, we pick a fixed real a_m for each natural number m (there is a unique choice), and define

$$\boxed{\Lambda_{m,k} = \Omega_m^k(U_k(a_m)),}$$

where

$$\boxed{\Omega_m = \omega_m^{(m+1)/2}.}$$

Thus,

$$\boxed{\Lambda_{m,k} = \Omega_m^k \frac{A^k(a_m) - B^k(a_m)}{A(a_m) - B(a_m)}}$$

are the generalized Fibonacci numbers (GFN); they are located "between" the number fields $Q(a_m, \omega_m)$ and $Q(\gamma_m, \omega_m)$. However, first observe that $\Lambda_{1,k} = F_k$, i.e., the $\Lambda_{m,k}$ are generalizations of Fibonacci numbers. From (1.5), we see that, for each choice of m, we have a family of GFNs which belong to the field $Q(a_m)$ and which have a functional equation generalizing that in $Q(a_1) = Q$, namely, one which generalizes the usual functional equation for the Fibonacci numbers. Moreover, we have the following interesting quasi-periodic behavior of these numbers, which is manifest only when $m > 1$.*

Theorem 3.4: Let $U_{i,j}(k) = U_{mk+j}(a_m), 0 \le j \le m$, m odd, then

$$\boxed{U_{mj}(k) \equiv F_{k+1}U_j(a_m) + (-1)^j F_k U_{m-j}(a_m) \bmod D_m(t),}$$

F_n, the n^{th} Fibonacci number, and D_m is as defined in Theorem 2.1.

Proof: Assume inductively that the theorem holds for $k < n$ and for $j - 1 \ge 1$. Assume that $U_{m,j}(k-1)$ satisfies the appropriate relation for $j = 0, \ldots, m-1$. We need to compute $U_{m,0}(k)$, but

$$\begin{aligned}
U_{m,0}(k) &= U_{mk}(t) = tU_{mk-1}(t) + U_{mk-2}(t)\\
&= tU_{m,m-1}(k-1) + dU_{m,m-2}(k-1)\\
&= t[F_k U_{m-1} + (-1)^{m-1}F_{k-1}U_1] +]F_k U_{m-2} + (-1)^{m-2}F_{k-1}U_2]\\
&= F_k[tU_{m-1} + U_{m-2}] + F_{k-1}[(-1)^{m-1}tU_1 + (-1)^{m-2}U_2]\\
&= F_k U_m + F_{k-1}[tU_1 - U_2] = F_k U_m,
\end{aligned}$$

since $U_1(t) = 1$, $U_1(t) = t$. But, if the theorem is correct, $U_{m,0}(k) = F_{k+1}U_0 + (-1)^0 F_k U_m = F_k U_m$. Thus, we have shown what is required. Next, we must show that the result holds for a fixed k and $j = 1, 2, \ldots, m-1$. Notice that the theorem is correct for $j = 0, \ldots, m-1$, $k = 0$, and for $j = 0$, $k = 1$. Suppose that it holds for $k < n$ and $j = 0, \ldots, m-1$ and for $k = n$ and $j = 0$. We want to show that it holds for $k = n$, $j = 1, \ldots, m-1$. So consider $U_{mj}(k)$, $k = n$, $1 \le j \le m-1$.

$$\begin{aligned}
U_{mj}(k) &= tU_{m,j-1}(k) + U_{m,j-2}(k)\\
&= t[F_{k+1}U_{j-1} + (-1)^{j-1}F_k U_{m-j+1}] + [F_{k+1}U_{j-2} + (-1)^{j-2}F_k U_{m-j+2}]\\
&= F_{k+1}[tU_{j-1} + U_{j-2}] + (-1)^{j-1}F_k[tU_{m-j+1} - U_{m-j+2}]\\
&= F_{k+1}U_j + (-1)^{j-1}F_k[tU_{m-j+1} - U_{m-j+2}]\\
&= F_{k+1}U_j + (-1)^{j-1}F_k[[tU_{m-j+1} - (tU_{m-j+1} + U_{m-j})]\\
&= F_{k+1}U_j + (-1)^j F_k U_{m-j}. \ \square
\end{aligned}$$

* We should point out that this is a special case of a phenomenon which always occurs in the context of a certain class of multiplicative arithmetic functions (see [9]).

The numbers for $m = 3$ are:

$$U_{3,3k} = -F_{k-1}\omega_3(1+a_3^2);\quad U_{3,3k+1} = F_k - F_{k-1}a_3;\quad U_{3,3k+2} = (F_k a_3 + F_{k-1})\omega_3^2.$$

4. THE ALGEBRAIC NUMBER FIELDS $Q(\gamma_m)$, $Q(\delta_m)$, $Q(a_m)$

We assume that m is odd and note that

Proposition 4.1: a_p, γ_p, δ_p, ω_p are units in the ring of integers of $Q(a_p)$.

Proof: $t^{2p} - t^p - 1$ is the minimum polynomial of $Q(\gamma_p)$. Both γ_p and δ_p satisfy this polynomial. Moreover, $a_p = -\omega_p(\gamma_p + \delta_p)$. Note that α and β clearly belong to $Q(\gamma_p)$. □

The most interesting result to come out of the ideas considered in this paper is the way in which the polynomials U_m and V_m provide the structural framework for the algebraic number fields determined by the numbers γ_m, δ_m, a_m. A first example of this fact is contained in the role that the polynomials D_m play. $D_m(t)$ is irreducible over Q for m odd. This can be proved by using earlier propositions and Eisenstein's criterion; however, the following proof is instructive.

Theorem 4.2: $\mathcal{F}_m = Q[t]/\langle D_m(t)\rangle$ is a field for odd m.

Proof: Let p be an odd prime.

Lemma 4.2.1: ***(a)*** $D_p(t)$ is a monic polynomial of degree p with constant term ± 1.

(b) p divides all interior coefficients of $D_p(t)$.

Proof of Lemma: (a) follows from (1.5) by induction and definition. For (b), we need to know that the "interior" coefficients of $D_p(t)$ are given by

$$\boxed{P_k(p+1) + P_{k-1}(p-1) = \binom{p-k-1}{k+1} + \binom{p-k-2}{k}.}$$

But this follows easily from (2.1), (2.2), and (2.5). Then it is straightforward to show that

$$P_k(p+1) + P_{k-1}(p-1) = \frac{(p-k-2)!}{(p-2k-2)!(k+1)!}p.$$

Since p is prime, hence is relatively prime to the denominator, p divides $P_k(p+1) + P_{k-1}(p-1)$. □

Thus, by a standard application of Eisenstein's lemma, $D_p(t)$ is irreducible over Q, so the theorem holds for the case $m = p$, p a prime. Thus, $\mathcal{F}_p$ is a field. We want to show that $\mathcal{F}_{np}$ is a field for any odd prime p and any natural number n. First, we prove a lemma which is of interest in its own right.

Lemma 4.2.2 (The Embedding Lemma): There is a natural embedding of the ring $\mathcal{F}_{p^{n-1}}$ in the ring $\mathcal{F}_{p^n}$.

Proof: It is convenient first to note that the ring $\mathcal{F}_m$ can be represented by elements of the form $\sum_{i=0}^{m-1} m_i a_m^i$, $m_i \in Q$, taken mod $D_m(t)$. Now we consider $(D_{p^{k-1}} \circ V_p)(a_{p^k})$.

$$(D_{p^{k-1}} \circ V_p)(a_{p^k}) = V_{p^{k-1}}(V_p(a_{a^k})) + (-1)^{(p+1)/2} = V_{p^k} a_{p^k} + (-1)^{(p+1)/2} = D_{p^k}(a_{p^k}) = 0.$$

Thus, $V_p(a_{p^k}) = a_{p^{k-1}}$. Now, $V_p(a_{p^k}) \in \mathcal{F}_{p^k}$. Since $a_{p^k} \in \mathcal{F}_{p^k}$, so does a copy of $a_{p^{k-1}}$. Since this element satisfies D_{p^k} and $\mathcal{F}_{p^{k-1}}$ consists of elements of the form $\sum_{i=0}^{p^{k-1}} m_i a_{p^{k-1}}$, so we have an embedding of $\mathcal{F}_{p^{k-1}}$ in $\mathcal{F}_{p^k}$ determined by the polynomials V_k. So assume inductively that $\mathcal{F}_{p^k}$ is a field for $k \le n$, and let I be maximal ideal in the Noetherian ring $\mathcal{F}_{p^k}$. $\mathcal{F}_{p^k}/I$ is a field, one which contains a copy of $\mathcal{F}_{p^{k-1}}$, so the degree of $\mathcal{F}_{p^k}/I$ (over Q) is $\ge p^{k-1}$. Now a_{p^k} is a unit, so $a_{p^k} \notin I$; thus, $a_{p^k} + I \in D_{p^k}/I$ and is not trivial. And so the degree of $D_{p^k}/I > p^{k-1}$, and thus the degree of $D_{p^k}/I = p^k$. Therefore, the minimum polynomial of $\mathcal{F}_{p^k}/I$ is a multiple of D_{p^k}, hence is equal to D_{p^k}, and so $I = O$, and $\mathcal{F}_{p^k}$ is a field. □

Thus, we have proved the theorem for m an odd prime power. This argument applied to $V_m(V_p(a_{mp}))$, $(m, p) = 1$, extends the result to $\mathcal{F}_{mp}$, $(m, p) = 1$. Thus, $\mathcal{F}_n$ is a field for all odd n.

Corollary 4.2.3: If m divides n, m and n both odd, then $\mathcal{F}_m$ is (isomorphic to) a subfield of $\mathcal{F}_n$ under the embedding determined by $(-1)^{(n-1)/2} V_m(V_k(a_{mk})) = a_m$, $n = mk$. □

Since $\gamma_m = \omega_m^{(m+1)/2} A(a_m)$, $\delta_m = \omega_m^{(m+1)/2} B(a_m)$, it follows that $\mathcal{F}_m < Q(a_m, \omega_m) < Q(\gamma_m, \omega_m)$. The last two fields are splitting fields. We thus have the following degree relations.

Theorem 4.3: $[Q(a_m):Q] = [\mathcal{F}_m : Q] = m$, $[Q(a_m, \omega_m) : \mathcal{F}_m] = \phi(m)$, $[Q(\gamma_m, \omega_m) : Q(a_m, \omega_m)] = 2$, where ϕ is the Euler totient function.

The following theorem is another illustration of how the polynomials U_m and V_m are involved in the structure of the fields $\mathcal{F}_m$.

Theorem 4.4: $\Delta[1, a_m, \ldots, a_m^{m-1}] = (-1)^{m(m-1)/2} m^m N U_m(a_m)$, is the norm of the algebraic number $U_m(a_m)$.

Proof: In any case, since $\frac{d}{dt}(V_m) = \frac{d}{dt}(D_m)$,

$$\Delta[1, a_m, \ldots, a_m^{m-1}] = (-1)^{m(m-1)/2} N\left(\frac{d}{dt}\right)(V_m)(a_m),$$

by (1.7), $d/dtV_m = mU_m$ and $N(mU_m(a_m)) = m^m N(U_m(a_m))$. □

Example: It follows from Theorem 4.4 that, when $m = 3$, $\Delta[1, a_3, a_3^2] = -3^3 \cdot 5$. This can be computed directly by using the representation of $\mathcal{F}_3$ determined by the minimal polynomial. Thus,

$$a_3 = \begin{vmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -3 & 0 \end{vmatrix}, \quad \text{and so} \quad 1 + a_3^2 = \begin{vmatrix} 1 & 0 & 1 \\ 1 & -2 & 0 \\ 0 & 1 & -2 \end{vmatrix},$$

from which it follows that

$$N\left(\frac{d}{dt} V(t)\bigg|_{t=a_3}\right) = N(3F_3(a_3)) = 3^3 \det(1 + A_3^2) = 3^3 \cdot 5.$$

So $\Delta = -3^3 \cdot 5$ as promised by the theorem. We can write $\Delta[1 \cdot a_m, \ldots, a_m^{m-1}]$ explicitly.

Theorem 4.5: $\Delta[1 \cdot a_m, \ldots, a_m^{m-1}] = (-1)^{m(m-1)/2} m^m \cdot 5^n$, $m = 2n+1$.

Proof: By Theorem 4.4, we need only compute $N(U_m(a_m)) = 5^n$. To do this, let $\lambda_1, \dots, \lambda_m$ be the m distinct conjugates of a_m with $a_m = \lambda_1$. Then

$$Nu_m(a_m) = \prod_{k=1}^{m} \frac{A^m(\lambda_k) - B^m(\lambda_k)}{R(\lambda_k)}$$

$$= \prod_{k=1}^{m} \frac{\gamma_{(k)}^m - \delta_{(k)}^m}{R(\lambda_k)} = \prod_{k=1}^{m} \frac{\gamma_{(k)}^m - \delta_{(k)}^m}{\gamma_{(k)} - \delta_{(k)}},$$

where $\gamma_{(k)}$ and $\delta_{(k)}$ are the conjugates of γ_m and δ_m.

$$\prod_{k=1}^{m} \frac{\gamma_{(k)}^m - \delta_{(k)}^m}{\gamma_{(k)} - \delta_{(k)}} = \prod_{k=1}^{m} \frac{(\alpha - \beta)^m}{\gamma_{(k)} - \delta_{(k)}}$$

$$= \frac{(\sqrt{5})^m}{\prod_1^m (\gamma_{(k)} - \delta_{(k)})} = \frac{5^n\sqrt{5}}{\prod_1^m (\gamma_{(k)} - \delta_{(k)})}.$$

Now,

$$\prod_1^m (\gamma_{(k)} - \delta_{(k)}) = \Pi\gamma_{(k)} - \Pi\delta_{(k)} + \sum_{s \ge 1} \gamma_{(k_1)} \cdots \gamma_{(k_s)} \delta_{(k_1)} \cdots \delta_{(k_s)}.$$

Since $\gamma_{(k)}$ satisfies $x^m - \alpha = 0$ and $\delta_{(k)}$ satisfies $x^m - \beta = 0$, $\Pi\gamma_{(k)} = \alpha$ and $\Pi\delta_{(k)} = \beta$, so $\Pi\gamma_{(k)} - \Pi\delta_{(k)} = \alpha - \beta = \sqrt{5}$. The remaining products are symmetric polynomials involving at least two symbols, but not all, so, from the equation satisfied by the γ's and δ's, are 0. □

The significance of the algebraic numbers a_m is now clear. To understand the fields $Q(\alpha_m)$ and $Q(\delta_m)$ and their normal extensions, it is sufficient to understand the fields $\mathscr{F}_m$ (and their normal extensions), for $Q(\gamma_m)$, for example, is an easily understood quadratic extension of $\mathscr{F}_m$. The role that the polynomial sequences U_m and V_m play in determining the structure in these fields is also clear, and surprising. The GFNs are integers in these fields, since a_m and ω_m are. So we are left with the standard questions: the class numbers, the maximal orders, units, primes, etc., of these fields (see, e.g., [11]). It is tempting to believe that, linked as these nonquadratic extensions are to a "base" field which is of the *Richaud-Degert* (R-D) type, some adaptation of the elegant methods used for R-D type fields might be found. Of course, the periodic nature of continued fraction expansions of quadratic irrationalities is an intriguing obstacle in the cases of degree greater than 2.

Some direct computations for small m are possible. We illustrate for $m = 3$. (When $m = 1$, the field is, of course, just $Q(\sqrt{5})$). Therefore, we should start at $m = 3$. (The theory for m even has much in common with the case of m odd, but also some significant differences that occur because the minimal polynomials need not have real roots. Moreover, the sequences $\{U_m\}$ and $\{V_m\}$ are markedly different for m even and for m odd. We postpone this discussion.)

A Computation for $\boldsymbol{m = 3}$**:** Using the faithful representation ρ for a_3 as in the illustration of Theorem 4.4,

$$\rho(a_3) = \begin{vmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -3 & 0 \end{vmatrix} = M,$$

and letting

$$\rho(k_0+k_1a_3+k_2a_3^2)=k_0I+k_1M+k_2M=\begin{vmatrix}k_0 & k_2 & k_1\\ k_1 & k_0-3k_2 & k_2-3k_1\\ k_2 & k_1 & k_0-3k_2\end{vmatrix}.$$

Then,

$\sum k_i a_3^i \in Z(a_m)$ is an algebraic integer iff $M(k_0, k_1, k_2)$ is an integer matrix;
$\sum k_i a_3^i \in Z(a_m)$ is a unit iff $M(k_0, k_1, k_2) = N(\sum k_i a_3^i) = \pm 1$.
$\sum k_i a_3^i \in Z(a_m)$ is a prime if det $M(k_0, k_1, k_2)$ is a rational prime (e.g., $1-a$ is a prime in $\mathcal{F}_3$).

We know that either a prime ideal in Z is a prime ideal in $\mathcal{F}_3$ or factors into two prime ideals. We can determine this for each prime ideal $\langle p\rangle$ by checking to see if t^3+t+1 is irreducible mod p. For example, 2 is a prime in $\mathcal{F}_3$, while 3 and 5 factor, 7 is prime. Since $\Delta_3(\mathcal{F}_3)=-3^3 5$, 3 and 5 ramify; 3 ramifies totally, $\langle 3\rangle=\langle 1-a\rangle^3$. The ramification index is 3, and the relative degree is 1. For 5, $\langle 5\rangle=\langle 4+a^2\rangle\langle 1+a^2\rangle$ with ramification numbers $e_1=1$ and $e_2=2$ and relative degrees $f_1=1$ and $f_2=1$. Using Minkowski's theorem, we can compute

$$h(\mathcal{F}_3)=\frac{4}{\pi}\frac{3!}{3^3}|\Delta(\mathcal{F}_3)|^{1/2}\le 2,$$

and so the class number of $\mathcal{F}_3$ is 1.

REFERENCES

1. M. Bicknell. "A Primer for Fibonacci Numbers–Part VII: Introduction to Fibonacci Polynomials and Their Divisibility Properties." *The Fibonacci Quarterly* **8.5** (1970):407-20.
2. B. G. S. Doman & J. K. Williams. "Fibonacci and Lucas Polynomials." *Math. Proc. Camb. Phil. Soc.* **90** (1981):385-87.
3. Günther Frei. "Binary Lucas and Fibonacci Polynomials, I." *Math. Nach.* **96** (1980):83-112.
4. P. Filipponi & A. F. Horadam. "Derivative Sequences of Fibonacci and Lucas Polynomials." In *Applications of Fibonacci Numbers* **4:**99-108. Dordrecht: Kluwer, 1991.
5. F. J. Galvez. "Novel Properties of Fibonacci and Lucas Polynomials." *Math. Proc. Camb. Phil. Soc.* **97** (1985):159-64.
6. Alan R. Glasson. "Remainder Formulas Involving Generalized Fibonacci and Lucas Polynomials." *The Fibonacci Quarterly* **33.3** (1995):268-72.
7. V. E. Hoggatt, Jr., & C. T. Long. "Divisibility Properties of Generalized Fibonacci Polynomials." *The Fibonacci Quarterly* **12.2** (1974):113-20.
8. Arnold Knopfmacher & M. E. Knopfmacher. "Mays Pierce Expansions of Ratios and Fibonacci and Lucas Numbers and Polynomials." *The Fibonacci Quarterly* **33.3** (1995):153-63.
9. T. MacHenry. "A Subgroup of the Group of Units in the Ring of Arithmetic Functions." *Rocky Mountain J. Math.* (to appear).
10. R. A. Mollin. *Quadratics.* Boca Raton, New York, London, Tokyo: CRC Press, 1996.
11. M. E. Pohst. "Three Principal Tasks of Computational Algebraic Number Theory." In *Number Theory and Applications* **265:**123-34. Ed. R. A. Mollin. Dordrecht: Kluwer, 1989.
12. Chi Zhang Zhou. "On the k^{th}-Order Derivative Sequences of Fibonacci and Lucas Polynomials." *The Fibonacci Quarterly* **34.5** (1996):394-408.

AMS Classification Numbers: 11A25, 11B39, 11R29, 11R04

❖❖❖