ON THE SOLUTIONS TO THE DIOPHANTINE EQUATION $x^2 + xy - y^2 = \pm D$, OR THE NUMBER OF FIBONACCI-TYPE SEQUENCES WITH A GIVEN CHARACTERISTIC

BRIAN PETERSON and V.E. HOGGATT, JR.
San Jose State University, San Jose, California 95192

In this paper we are concerned with a question that has already been answered, involving Fibonacci-type sequences and their characteristic numbers. We are only interested in primitive sequences (consecutive pairs of terms have no common factors) and for these sequences we ask: What numbers can be the characteristic of a sequence, and given such a number, how many sequences have it?

Thoro [1] has shown that D may be the characteristic of a sequence if and only if D has prime power decomposition

$$D = 5^e p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} ,$$

where $e = 0$ or 1 and $p_i = 10m \pm 1$ for all i, while Levine [2] has shown that for such D, there are exactly 2^n primitive sequences possessing it. Levine's proof involves the use of quadratic fields and rings of integers in such fields.

Our purpose, here partly fulfilled, is to construct an elementary proof. In this paper, we show the ideas of our argument, and the difficulties encountered.

In what follows, F_n and L_n are the n^{th} Fibonacci and Lucas numbers, respectively, while H_n, H_n^*, A_n, B_n, etc., will represent the n^{th} term of some general Fibonacci-type sequence. It can be shown that any sequence has a "pivotal" element, such that it and all of the elements after (or before) it are of the same sign, which we take positive when convenient, while the element before (or after) it is of the opposite sign and all the elements before it have alternating signs. With the exception of the Fibonacci sequence $\{\cdots, 1, 0, 1, 1, 2, \cdots\}$, we will always assume that for a sequence

$$\{H_n\}_{n=-\infty}^{\infty} ,$$

H_0 is the pivotal element. Finally, if $\{H_n\}$ is a sequence, then by $\{\bar{H}_n\}$ we will mean the conjugate sequence whose terms are given by

$$\bar{H}_n = (-1)^n H_{-n} .$$

Henceforth, when we say sequence, unless otherwise stated, we will mean Fibonacci-type sequence.

We begin by stating the identity

$$F_{m+1}F_{n+1} + F_m F_n = F_{m+n+1} , \tag{1}$$

which can be proved by induction on either m or n. There are several similar identities:

$$L_{m+1}F_{n+1} + L_m F_n = L_{m+n+1} \tag{2}$$

$$H_{m+1}F_{n+1} + H_m F_n = H_{m+n+1} \tag{3}$$

$$L_{m+1}L_{n+1} + L_m L_n = 5F_{m+n+1} \tag{4}$$

and in general,

$$H_{m+1}H_{n+1}^* + H_m H_n^* = G_{m+n+1} \tag{5}$$

gives the terms of a sequence $\{G_n\}$. What we have, then, is a way of combining pairs of sequences to obtain a new sequence, a type of multiplication of sequences. We will see shortly that this operation is commutative and associative, as may already be apparent.

We will need to recall a few notions concerning sequences.

For any sequence, there is a positive number C, called the characteristic number for the sequence, such that

$$H_{n-1}H_{n+1} - H_n^2 = \pm C, \tag{6}$$

where the sign varies according as n is even or odd.

Also, for any sequence, there is a function which generates the terms with non-negative subscripts, given by

$$\frac{H_0 + H_{-1}x}{1 - x - x^2} = \sum_{n=0}^{\infty} H_n x^n. \tag{7}$$

Recall, too, that given any two sequences $\{H_n\}$ and $\{H_n^*\}$, we can form what is called the convolution of the sequences, given by the sequence

$$\{C_n\}_{n=0}^{\infty}$$

which is not Fibonacci-type and which has terms given by

$$\begin{aligned} &C_0 = H_0H_0^*, \quad C_1 = H_1H_0^* + H_0H_1, \quad C_2 = H_2H_0^* + H_1H_1^* + H_0H_2^* \\ &\cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \\ &C_n = H_nH_0^* + H_{n-1}H_1^* + \cdots + H_1H_{n-1}^* + H_0H_n^*. \end{aligned} \tag{8}$$

The terms of $\{C_n\}$ satisfy the recurrence

$$C_{n+4} - 2C_{n+3} - C_{n+2} + 2C_{n+1} + C_n = 0, \tag{9}$$

and are generated by the product of the generating functions for $\{H_n\}$ and $\{H_n^*\}$,

$$\frac{(H_0 + H_{-1}x)(H_0^* + H_{-1}^*x)}{(1 - x - x^2)^2} = \sum_{n=0}^{\infty} C_n x^n. \tag{10}$$

We will now see that the convolution of the sequences $\{H_n\}$ and $\{H_n^*\}$ is closely related to the sequence $\{G_n\}$ given by Eq. (5).

For a Fibonacci-type sequence $\{A_n\}$ we have

$$A_{n+2} - A_{n+1} - A_n = 0. \tag{11}$$

The sequence $\{C_n\}$ above does not satisfy Eq. (11), but if we let

$$C_{n+2} - C_{n+1} - C_n = \Delta_n \tag{12}$$

then we observe that

$$\begin{aligned} \Delta_{n+2} - \Delta_{n+1} - \Delta_n &= (C_{n+4} - C_{n+3} - C_{n+2}) - (C_{n+3} - C_{n+2} - C_{n+1}) - (C_{n+2} - C_{n+1} - C_n) \\ &= C_{n+4} - 2C_{n+3} - C_{n+2} + 2C_{n+1} + C_n = 0. \end{aligned}$$

So the $\{\Delta_n\}$ forms a Fibonacci-type sequence. Since two adjacent terms of a sequence determine the sequence, we have only to look at Δ_0 and Δ_1 to know all about $\{\Delta_n\}$. We will see that $\Delta_0 = G_1$ and $\Delta_1 = G_2$.

From Eq. (8) and then (5), we see that

$$\begin{aligned} \Delta_0 &= C_2 - C_1 - C_0 = (H_2H_0^* + H_1H_1^* + H_0H_2^*) - (H_1H_0^* + H_0H_1^*) - (H_0H_0^*) \\ &= (H_2 - H_1 - H_0)H_0^* + (H_1 - H_0)H_1^* + H_0H_2^* = (0)H_0^* + (H_{-1})H_1^* + H_0H_2^* = G_1, \end{aligned}$$

and, since

$$C_3 = H_3H_0^* + H_2H_1^* + H_1H_2^* + H_0H_3^*,$$

$$\begin{aligned} \Delta_1 &= C_3 - C_2 - C_1 = (H_3 - H_2 - H_1)H_0^* + (H_2 - H_1 - H_0)H_1^* + (H_1 - H_0)H_2^* + H_0H_3^* \\ &= (0)H_0^* + (0)H_1^* + (H_{-1})H_2^* + H_0H_3^* = G_2. \end{aligned}$$

Thus, we have

$$G_n = C_{n+1} - C_n - C_{n-1}, \tag{13}$$

which can be interpreted in terms of generating functions. Using Eq. (10), we have

$$(1-x-x^2)\frac{(H_0+H_{-1}x)(H_0^*+H_{-1}^*x)}{(1-x-x^2)^2}=\sum_{n=0}^{\infty}C_nx^n=\sum_{n=1}^{\infty}C_{n-1}x^n-\sum_{n=2}^{\infty}C_{n-2}x^n$$

$$=C_0+(C_1-C_0)x+\sum_{n=2}^{\infty}(C_n-C_{n-1}-C_{n-2})x^n\,,$$

or,

$$\frac{(H_0+H_{-1}x)(H_0^*+H_{-1}^*x)}{1-x-x^2}=C_0+(C_1-C_0)x+\sum_{n=2}^{\infty}G_{n-1}x^n\,. \tag{14}$$

Thus, we see that, if we simply multiply the numerators of the generating functions for $\{H_n\}$ and $\{H_n^*\}$, we obtain, except for the first couple of terms, a generating function for $\{G_n\}$.

From this, it follows immediately that our operation of multiplying sequences is commutative and associative, since multiplication of polynomials is commutative and associative.

Next, we will show that, when we multiply sequences, the product of their characteristic numbers give the characteristic of the product. Unfortunately, we have no neat way to show this, so we indicate the steps in the rather messy but elementary calculation. If we let

$$\{A_n\}=\{\cdots,a,b,a+b,\cdots\}\qquad\text{and}\qquad\{C_n\}=\{\cdots,c,d,c+d,\cdots\},$$

then their product, which we denote $\{AC_n\}$, has

$$\{AC_n\}=\{\cdots,bd+ac,(a+b)d+bc,(a+2b)d+(a+b)c,\cdots\}.$$

Ignoring the question of sign, $\{A_n\}$ has characteristic a^2+ab-b^2, and $\{C_n\}$ has characteristic c^2+cd-d^2. We compute the characteristic of $\{AC_n\}$, and find it is the product of these, as follows:

$$[bd+ac][(a+2b)d+(a+b)c]-[(a+b)d+bc]^2$$

$$=[abd^2+2b^2d^2+abcd+b^2cd+a^2cd+2abcd+a^2c^2+abc^2]-[a^2d^2+b^2d^2+2abd^2+b^2c^2+2abcd+2b^2cd]$$

$$=a^2c^2+a^2cd-a^2d^2+abc^2+abcd-abd^2-b^2c^2-b^2cd+b^2d^2=(a^2+ab-b^2)(c^2+cd-d^2)\,.$$

Thus, the characteristic of the product is the product of the characteristics.

These are the tools we wish to use in our argument, which rests upon something we have so far been unable to show with an elementary proof. We want to show that, for a prime $p=10m\pm1$, exactly two sequences have p as their characteristic, and that these are conjugate to one another. Then we would like to show that these are the atoms from which we can build the whole universe of sequences.

Suppose that we are successful in dealing with this basic problem of showing that exactly two sequences correspond to a prime $p=10m\pm1$. Then, we have several lemmas that show that we can build from the sequences corresponding to prime characteristics.

Lemma 1. The product of a sequence $\{A_n\}$ and its conjugate $\{\bar{A}_n\}$ is not primitive, unless it is the sequence $\{F_n\}$.

Proof. Let $a, b, c > 0$ and let

$$\{A_n\}=\{\cdots,-a,b,c,\cdots\};$$

i.e., b is the pivotal element of $\{A_n\}$. Then,

$$\{A_n\}=\{\cdots,-c,b,a,\cdots\}\qquad\text{and}\qquad A_0\bar{A}_1+A_{-1}\bar{A}_0=ba+(-a)b=0,$$

so $\{A\bar{A}_n\}$ has a zero. But, only a multiple of the Fibonacci sequence can have a zero. Since the characteristic of $\{A\bar{A}_n\}$ is the product of the characteristics of $\{A_n\}$ and $\{\bar{A}_n\}$, which are easily seen to be the same, we see that $\{A\bar{A}_n\}=\{cF_n\}$, where c is the characteristic of $\{A_n\}$. Since $c\neq1$ as long as $\{A_n\}\neq\{F_n\}$, we see that $\{A\bar{A}_n\}$ is not primitive.

Lemma 2. If we write $\{A_n^m\}$ for the product $\{AAA\cdots A_n\}$ where A appears m times, then if

$$\frac{a + bx}{1 - x - x^2} = \sum_{n=0}^{\infty} A_n x^n$$

so that

$$(a + bx)^m/(1 - x - x^2)$$

generates $\{A_n^m\}$ except for the first few terms, then we can write

$$\frac{(a + bx)^m}{1 - x - x^2} = p_{m-1}(x) + \frac{(A_m + B_m x)x^{m-1}}{1 - x - x^2} ,$$

where $P_{m-1}(x)$ is a polynomial of degree $m - 1$ and B_m, A_m are consecutive terms of $\{A_n^m\}$.

Proof. We delete. The idea is to expand $(a + bx)^m$ and then divide by $(1 - x - x^2)$ and get the remainder, which is linear.

Lemma 3. Given $\{A_n\}$ and all its powers $\{A_n^m\}$ as above, the A_m's and B_m's introduced there satisfy the following recurrences:

$$A_{m+1} = (a + b)A_m + aB_m$$
$$B_{m+1} = aA_m + bB_m$$
$$A_{m+2} = (a + 2b)A_{m+1} + cA_m$$
$$B_{m+2} = (a + 2b)B_{m+1} + cB_m ,$$

where $c = a^2 - ab - b^2$ is the characteristic of $\{A_n\}$.

Proof. If

$$\frac{(a + bx)^m}{1 - x - x^2} = p_{m-1}(x) + \frac{(A_m + B_m x)x^{m-1}}{1 - x - x^2}$$

then

$$\begin{aligned}
\frac{(a + bx)^{m+1}}{1 - x - x^2} &= (a + bx)p_{m-1}(x) + \frac{(a + bx)(A_m + B_m x)}{1 - x - x^2} \\
&= p'_m(x) + \frac{(aA_m + (bA_m + aB_m)x + bB_m x^2)x^{m-1}}{1 - x - x^2} \\
&= p'_m(x) + x^{m-1}\left[aA_m + \frac{((a + b)A_m + aB_m)x + (aA_m + bB_m)x^2}{1 - x - x^2} \right] \\
&= p_m(x) + x^m \left[\frac{((a + b)A_m + aB_m) + (aA_m + bB_m)x}{1 - x - x^2} \right] \\
&= p_m(x) + \frac{(A_{m+1} + B_{m+1}x)x^m}{1 - x - x^2}
\end{aligned}$$

and

$$A_{m+1} = (a + b)A_m + aB_m$$
$$B_{m+1} = aA_m + bB_m .$$

Now, using these, we have

$$\begin{aligned}
A_{m+2} &= (a + b)A_{m+1} + aB_{m-1} = (a + b)A_{m+1} + a(aA_m + bB_m) \\
&= (a + b)A_{m+1} + a^2A_m + b(aB_m) = (a + b)A_{m+1} + a^2A_m + b(A_{m+1} - (a + b)A_m) \\
&= (a + 2b)A_{m+1} + (a^2 - ab - b^2)A_m ,
\end{aligned}$$

$$\begin{aligned} B_{m+2} &= aA_{m+1} + bB_{m+1} \\ &= a((a+b)A_m + aB_m) + bB_{m+1} \\ &= (a+b)(aA_m) + a^2B_m + bB_{m+1} \\ &= (a+b)(B_{m+1} - bB_m) + a^2B_m + bB_{m+1} \\ &= (a+2b)B_{m+1} + (a^2 - ab - b^2)B_m . \end{aligned}$$

Lemma 4. If a sequence is primitive, then its product with itself either is primitive or has 5 as a factor.

Proof. We have a sequence generated by

$$(a+bx)/(1-x-x^2),$$

where $(a,b) = 1$. Note that (a,b) means the greatest common divisor of a and b, and that for a sequence to be primitive is to say that any pair of consecutive terms are relatively prime. Now,

$$\frac{(a+bx)^2}{1-x-x^2} = a^2 + \frac{[(a^2+2ab) + (a^2+b^2)x]x}{1-x-x^2}$$

so we must consider (a^2+2ab, a^2+b^2). We suppose that some prime p divides both a^2+2ab and a^2+b^2.

If $p \mid a(a+2b)$ and $p \mid (a^2+b^2)$, then

$$p \mid (a^2+2ab-a^2-b^2) = 2ab - b^2, \qquad \text{or,} \qquad p \mid b(2a-b).$$

If $p \mid a$, then since $p \mid (a^2+b^2)$, $p \mid b$, and if $p \mid b$, then $p \mid a$ for the same reason. But, $(a,b) = 1$, so p cannot divide both a and b, and $p \mid (a+2b)$, $p \mid (2a-b)$. So,

$$p \mid [(a+2b) + 2(2a-b)] = 5a,$$

and $p \mid 5$ because p does not divide a and p is a prime. Then, we may conclude that (a^2+2ab, a^2+b^2) is a power of 5. But, we will show that (a^2+2ab, a^2+b^2) must divide D, the characteristic of our given primitive sequence. Since D contains at most one factor of 5, we will have the desired result.

Note that $D = \pm(a^2 - ab - b^2)$. we suppose that $d \neq 1$ and that $d \mid (a^2+2ab)$, $d \mid (a^2+b^2)$. Then,

$$d \mid [a(a^2+2ab) - (a+b)(a^2+b^2)] = a^2b - ab^2 - b^3 = Db$$

and

$$d \mid [b(a^2+2ab) - a(a^2+b^2)] = -a^3 + a^2b + ab^2 = -Da.$$

We let $(D,d) = d'$. Then $d/d' \mid Db/d'$ and $d/d' \mid Da/d'$, but since $(d/d', D/d') = 1$, $d/d' \mid b$ and $d/d' \mid a$, and since $(a,b) = 1$, $d/d' = 1$ or $d = d'$ so that, since $(D,d) = d$, we see that $d \mid D$.

Lemma 5. If $\{H_n\}$ has starting pair b,a and $(a,b) = 1$, then

$$(a^2+2ab, a^2+b^2) = 5$$

if and only if $\{H_n\} = \{H'L_n\}$; i.e., $\{H_n\}$ is the product of some $\{H'_n\}$ with the Lucas sequence.

Proof. The if part is easy. Let $\{H_n\} = \{H'L_n\}$. Then

$$\{H_n^2\} = \{H'LH'L_n\} = \{H'^2L_n^2\}.$$

But, $\{L_n^2\} = \{5F_n\}$ so

$$\{H_n^2\} = \{H_n'^2\} \cdot \{5F_n\} = \{5H_n'^2\}$$

and clearly 5 divides each term, including a^2+2ab and a^2+b^2.

Now, for the only if part. We let $(a,b) = 1$ and

$$(a^2+2ab, a^2+b^2) = 5.$$

Since $5 \mid (a^2+2ab)$ and $5 \mid (a^2+b^2)$,

$$5 \mid [(a^2+b^2) - (a^2+2ab)] = b^2 - 2ab.$$

Now,

$$5 \mid a(a + 2b) \qquad \text{and} \qquad 5 \mid b(b - 2a).$$

If $5 \mid a$, then since $5 \mid (a^2 + b^2)$, $5 \mid b$, and if $5 \mid b$, then $5 \mid a$ for the same reason. So, 5 cannot divide both a and b, and $5 \mid (a + 2b) = 5M$, $5 \mid (b - 2a) = 5M'$, so $a = M + 2M'$ and $b = 2M - M'$.

Now we set up the system of equations

$$a = rL_{k+1} + sL_k$$
$$b = rL_k + sL_{k-1}$$

which we know has solutions. We will show that r and s are integers which will complete the proof of Lemma 5. We use Cramer's rule.

$$r = \frac{\begin{vmatrix} a & L_k \\ b & L_{k-1} \end{vmatrix}}{\begin{vmatrix} L_{k+1} & L_k \\ L_k & L_{k-1} \end{vmatrix}} = \frac{\begin{vmatrix} M + 2M' & L_k \\ 2M - M' & L_{k-1} \end{vmatrix}}{(-1)^{k+1}5} = \frac{(M + 2M')L_{k-1} + (M' - 2M)L_k}{(-1)^{k+1}5}$$

$$= \frac{(2L_{k-1} + L_k)M' + (L_{k-1} - 2L_k)M}{(-1)^{k+1}5} = \frac{5F_kM' - 5F_{k-1}M}{(-1)^{k+1}5}$$

$$= (-1)^{k+1}(F_kM' - F_{k-1}M) \quad .$$

Similarly, s is found as

$$s = \frac{\begin{vmatrix} L_{k+1} & a \\ L_k & b \end{vmatrix}}{\begin{vmatrix} L_{k+1} & L_k \\ L_k & L_{k-1} \end{vmatrix}} = (-1)^{k+1}(F_kM - F_{k+1}M'),$$

so that we see both r and s are integers.

Lemma 6. If $(A_k, B_k) = 1$ and $(A_{k+1}, B_{k+1}) = 1$, then $(A_{k+2}, B_{k+2}) = 1$.

Proof. We let $p \mid A_{k+2}$ and $p \mid B_{k+2}$, p a prime. Then, certainly p divides the characteristic of the sequence

$$\{\cdots, B_{k+2}, A_{k+2}, \cdots\},$$

and since this is just the $(k + 2)^{nd}$ power of the characteristic of $\{\cdots, b, a, \cdots\}$ and p is a prime,

$$p \mid D = a^2 - ab - b^2 .$$

Now, since

$$A_{k+2} = (a + 2b)A_{k+1} + DA_k$$
$$B_{k+2} = (a + 2b)B_{k+1} + DB_k$$

we have that

$$p \mid (a + 2b)A_{k+1} \qquad \text{and} \qquad p \mid (a + 2b)B_{k+1} .$$

If p does not divide $(a + 2b)$, then $p \mid A_{k+1}$ and $p \mid B_{k+1}$, but $(A_{k+1}, B_{k+1}) = 1$, so $p \mid (a + 2b)$. But, we can show that

$$(a + 2b, D) = 1.$$

Certainly $(a, D) = 1$ because anything thad divides both a and D must divide b and $(a, b) = 1$. So,

$$(a + 2b, D) = (a(a + 2b), D) = (a^2 + 2ab, a^2 - ab - b^2).$$

If

$$p \mid (a^2 + 2ab) \qquad \text{and} \qquad p \mid (a^2 - ab - b^2),$$

then

$$p \mid (3ab + b^2) = b(3a + b)$$

and since p does not divide b, we must have $p \mid (3a + b)$ so $p \mid (6a + 2b)$. Now, since $p \mid (a + 2b)$, we see that $p \mid 5a$ and

since $p \nmid a$, $p \mid 5$, or, $p = 5$.

If $5 \mid A_{k+2}$ and $5 \mid B_{k+2}$, then $5 \mid D^{k+2}$, the characteristic of $\{ \cdots, B_{k+2}, A_{k+2}, \cdots \}$. But then $5 \mid D$ and $25 \mid D^2$. Thus, D^2 cannot be the characteristic of a primitive sequence (borrowing Thoro's result [1]). So, we may have had $(a,b) = 1$, but we would not have had

$$(a^2 + 2ab, a^2 + b^2) = 1.$$

Thus, nor would we have had $(A_{k+1}, B_{k+1}) = 1$. So we see that $(a + 2b, D) = 1$, and thus $(A_{k+2}, B_{k+2}) = 1$.

Notice that Lemma 6 shows that if a primitive sequence is not a Lucas mixture, then all of its powers are primitive. Our final sequence building lemma is

Lemma 7. If $\{ A_n \}$ has starting pair b,a with $(a,b) = 1$, and $\{ C_n \}$ has starting pair d,c with $(c,d) = 1$, and if $(D_1, D_2) = 1$, where $D_1 = a^2 - ab - b^2$ and $D_2 = c^2 - cd - d^2$, then $\{ AC_n \}$ is primitive.

Proof. $\{ AC_n \}$ is generated by

$$\frac{(a + bx)(c + dx)}{1 - x - x^2} = ac + \frac{[(ad + bc + ac) + (bd + ac)x]x}{1 - x - x^2} .$$

We must show that

$$(ad + bc + ac, bd + ac) = 1.$$

We let $p \mid (ad + bc + ac)$ and $p \mid (bd + ac)$. Then

$$p \mid [d(ad + bc + ac) - c(bd + ac)] = -a(c^2 - cd - d^2) = -aD_2$$

and

$$p \mid [b(ad + bc + ac) - a(bd + ac)] = -c(a^2 - ab - b^2) = -cD_1 .$$

Also,

$$p \mid [(ad + bc + ac) - (bd + ac)] = ad + bc - bd,$$

so

$$p \mid [c(ad + bc - bd) - d(bd + ac)] = b(c^2 - cd - d^2) = bD_2$$

and

$$p \mid [a(ad + bc - bd) - b(bd + ac)] = d(a^2 - ab - b^2) = dD_1 .$$

Thus we have that $p \mid aD_2$ and $p \mid bD_2$, and since it is impossible for p to divide both a and b, $p \mid D_2$. Likewise, $p \mid D_1$. But this cannot be, since $(D_1, D_2) = 1$. So, $\{ AC_n \}$ is primitive.

Note that, while Lemma 7 tells that, given a pair of primitive sequences with characteristics C_1 and C_2 relatively prime, we can construct a sequence with characteristic C_1C_2 that is also primitive, it does not say that, given two distinct pairs of sequences, their products are different.

There is also the question of whether, given a sequence with characteristic C_1C_2, it can be factored into a product of sequences with characteristics C_1 and C_2. This question corresponds to the problem of unique factorization in integral domains. In Levine's proof [2], he was able to use the well-known fact that factorization is unique in a certain integral domain, the "algebraic integers" in the algebraic number field $Q(\alpha)$, the rational numbers extended by $\alpha = (1 + \sqrt{5})/2$. We have so far been unable to show that we have unique factorization by means similar to those we have employed above.

As for the problem of knowing that exactly two sequences correspond to any prime characteristic $p = 10m \pm 1$, we have at least shown where to look for sequences having a given characteristic.

Lemma 8. If $\{ H_n \}$ has characteristic C, then $\{ H_n \}$ has a term in the interval $-\sqrt{C} \leq x \leq \sqrt{C}$.

Proof. We suppose that $\{ H_n \}$ has no terms in the interval $-\sqrt{C} \leq x \leq \sqrt{C}$. Then let H_k be the first term greater than $\sqrt{C}$. We ask, where does H_{k+1} lie? If $H_{k+1} < 0$, then by assumption $H_{k+1} < -\sqrt{C}$, and, in fact,

$$H_{k+1} < -(H_k + \sqrt{C})$$

or else H_{k+2} will be in the interval $-\sqrt{C} \leq x \leq \sqrt{C}$. If $H_{k+1} \geq 0$, then $H_{k+1} > \sqrt{C}$ and, in fact, $H_{k+1} > 2H_k$ or else H_{k-1} will be less than or equal to H_k and yet non-negative. This cannot be, because if $H_{k-1} < H_k$, then

$$-\sqrt{C} \leq H_{k-1} \leq \sqrt{C},$$

and if $H_{k-1} = H_k$, then $H_{k-2} = 0$ and 0 is in the interval.

So, in Case 1, where $H_{k+1} < 0$, we have

$$H_{k+1} < -(H_k + \sqrt{C}),$$

but all we will use is $|H_{k+1}| > |H_k|$. We let

$$H_k = a, \quad H_{k+1} = -b, \quad b > a > 0;$$

then $H_{k+2} = a - b < 0$. Since

$$H_k H_{k+2} - H_{k+1}^2 = a^2 - ab - b^2 < 0,$$

we see that

$$a^2 - ab - b^2 = -C, \quad \text{or,} \quad C = b^2 + ab - a^2.$$

Now, since $a < b$, we have

$$a < b$$
$$2a < 3b$$
$$2a^2 < 3ab$$
$$a^2 - 2ab + b^2 < b^2 + ab - a^2 = C$$
$$H_{k+2}^2 < C$$

or $|H_{k+2}| < \sqrt{C}$, and H_{k+2} is in $-\sqrt{C} \leq x \leq \sqrt{C}$.

Now, in Case 2, where $H_{k+1} \geq 0$, we have $H_{k+1} > 2H_k$. We let

$$H_k = a, \quad H_{k+1} = 2a + b,$$

where $a, b > 0$. Then $H_{k-1} = a + b$, and since

$$H_{k-1} H_{k+1} - H_k^2 = (a + b)(2a + b) - a^2 = a^2 + 3ab + b^2 > 0,$$

we have

$$C = a^2 + 3ab + b^2.$$

But then $H_k^2 < C$ because

$$C - H_k^2 = 3ab + b^2 > 0,$$

so $|H_k| < \sqrt{C}$, contrary to assumption. We are forced to conclude that $\{ H_n \}$ has a term in the interval $-\sqrt{C} \leq x \leq \sqrt{C}$.

Lemma 8 tells us where to look. Now we only have to know what we are looking for. Finding a sequence with characteristic C is the same as finding a solution to the diophantine equation

$$y^2 + xy - x^2 = \pm C,$$

because then $y, x, x + y$ will be consecutive terms of a sequence with characteristic C. We convert this equation to an equivalent one as follows:

(15)
$$y^2 + xy - x^2 = \pm C$$
$$4y^2 + 4xy - 4x^2 = \pm 4C$$
$$4y^2 + 4xy + x^2 - 5x^2 = \pm 4C$$
$$(2y + x)^2 - 5x^2 = \pm 4C$$

(16)
$$Y^2 - 5X^2 = \pm 4C$$

If y and x solve (15), then $2y + x$ and x solve (16). If Y and X solve (16), then $(Y - X)/2$ and X solve (15). (Note that $(Y - X)/2$ must be an integer since Y and X must be of the same parity to solve (16).)

If y and x solve (15), then $y = H_{k-1}$, $x = H_k$ give a sequence with characteristic C. Then

$$2y + x = 2H_{k-1} + H_k = H_{k-1} + H_{k+1}.$$

This is often called the generalized Lucas number, corresponding to the sequence $\{H_n\}$, and is written

$$H_{k-1} + H_{k+1} = \mathfrak{L}_k .$$

Now our problem is reduced to that of looking for solutions to (16) with $0 \leq X \leq \sqrt{C}$. That is, we need not consider $-\sqrt{C} \leq X \leq 0$, because the only X term in (16) is a square term.

If we find a solution X_0, it has a corresponding Y_0. But this Y_0 may be taken to be positive or negative. Also, there is possibly a Y_0^*, different from Y_0 numerically, that also corresponds to X_0. In this event, we would have that (X_0, Y_0) solves (16) for $+4C$, and (X_0, Y_0^*) with the $-4C$, or vice-versa. So, with a given X_0, there may be four Y's that correspond, but no more.

Given a solution (X_0, Y_0), we can obtain a sequence by letting

$$H_k = X_0, \qquad H_{k-1} = (Y_0 - X_0)/2 .$$

Also, any sequence containing X_0 and having characteristic C is obtainable in this way. To see this, we let $A_k = X_0$, and observe that $(A_k, 2A_{k-1} + A_k)$ solves (16), so that $2A_{k-1} + A_k$ was one of the (possibly four) Y's that went with X_0. Then we would have set

$$H_k = A_k, \qquad H_{k-1} = [(2A_{k-1} + A_k) - A_k]/2 = A_{k-1} .$$

As for the choice of (X_0, Y_0) or $(X_0, -Y_0)$ to construct a seuqence, we will obtain a sequence or its own conjugate. By taking (X_0, Y_0), we obtain

$$H_k = X_0, \qquad H_{k-1} = (Y_0 - X_0)/2,$$

so $H_{k+1} = (Y_0 + X_0)/2$. By taking $(X_0, -Y_0)$, we obtain

$$\overline{H}_k = X_0, \qquad \overline{H}_{k-1} = (-Y_0 - X_0)/2 = -H_{k+1} ,$$

so $\{\overline{H}_n\}$ is conjugate to $\{H_n\}$.

Similarly, if we take $(-X_0, Y_0)$ or $(-X_0, -Y_0)$, we get nothing new.

As for the choice between (X_0, Y_0) and (X_0, Y_0^*), at this point we have to say try them both. We believe that this still yields the same sequence, but as yet have no proof. This corresponds to situations in which the same number (up to absolute value) occurs twice in a sequence; for example, $\cdots, -7, 5, -2, 3, 1, 4, 5, 9, \cdots$ has two 5's.

At any rate, the problem of finding sequences with a given characteristic is reduced to that of finding solutions in a bounded interval to a particular diophantine equation.

REFERENCES

1. Dmitri E. Thoro, "A Diophantine Algorithm," (Abstract) *American Mathematical Monthly,* Vol. 71, No. 3, June-July, 1964, pp. 716–717.
2. Eugene Levine, "Fibonacci Sequences with Identical Characteristic Values," *The Fibonacci Quarterly,* Vol. 6, No. 5 (Nov. 1968), pp. 75–80).

★★★★★★