ON THE MULTIPLICATION OF RECURRENCES

PAUL A. CATLIN
Ohio State University, Columbus, Ohio 43210

In this note we shall consider recurrences of the form

$$A_{n+2} = A_{n+1} + A_n \ , \tag{1}$$

with initial values A_0 and A_1. The special case $A_0 = 0,\ A_1 = 1$ in (1) is the well known Fibonacci series (F_n), and $A_0 = 2,\ A_1 = 1$ is the Lucas series (L_n). The integer $N(A) = A_1^2 - A_0A_2$ is the *norm* (also known as the *characteristic number*) of (1). When recurrences (A_n) and (B_n) are multiplied (the multiplication of recurrences, which is defined below, was developed in [5]), we have that $N(A)N(B) = N(AB)$. This multiplicative property is the justification of the use of the word norm. In this paper, we shall derive some basic properties of recurrences under multiplication. Our main result will be that recurrences can be factored uniquely (up to order and sign) into recurrences whose norms are prime.

Let $A_0^* = A_0,\ A_1^* = A_0 - A_1$. The recurrence (A_n^*), obtained by using A_0^* and A_1^* as initial values in (1), will be called the *dual* recurrence of (A_n), and the asterisk will be used to denote dual recurrences. The notion of dual recurrences was introduced in [3]. It may be shown by induction that

$$A_n^* = F_{n+1}A_0^* - F_nA_1^* \ . \tag{2}$$

$t(A_n)$ will denote the *scalar product* (taken term-wise) of an integer t and (A_n). If $(A_0, A_1) = t > 1$, we can express the recurrence as a scalar product $t(B_n) = (A_n)$, where $tB_i = A_i$ for all i. It is only necessary to consider such reduced recurrences.

We define the *product* $(A_n)(B_n)$ of two recurrences to be the recurrence (C_n) (of the form (1)) such that

$$C_1 - aC_0 = (A_1 - aA_0)(B_1 - aB_0). \tag{3}$$

where a is a zero of $x^2 - x = 1$, the characteristic polynomial of (1) (a is adjoined to the integers, and (3) is an equation in the extension). It follows (see [5]) that

$$C_{m+n} = A_mB_{n+1} + A_{m+1}B_n - A_mB_n \ , \tag{4}$$

and

$$C_{m+n+1} = A_{m+1}B_{n+1} + A_mB_n \ . \tag{5}$$

As stated before (and in [5]), $N(A)N(B) = N(C)$.

We point out that the value of $N(A)$ changes only in sign as the starting point A_0 of the recurrence (A_n) is translated one term at a time: the value of $N(A) = A_1^2 - A_0A_2$ alternates in sign. This follows from the identity

$$(A_{n+1})^2 - A_nA_{n+2} = (-1)^nN(A) \ , \tag{6}$$

which may be proved by induction. Henceforth, we shall disregard the sign when we discuss the norm; we shall only use its absolute value. Also, the signs of terms of (A_n) will be disregarded in the sense that (A_n) and $-(A_n)$ will be considered equivalent. Thus, for the Fibonacci and Lucas series, we have that $N(F) = 1$ and $N(L) = 5$.

It has been shown (see [1]) that a recurrence other than (F_n) can be translated so that $|A_0| > |A_1|$, and that this representation is unique. For the purposes of this paper, however, we shall make no such assumption.

It follows from (4), (5) and the definitions of the norm and dual recurrences that

$$(A_n)(A_n^*) = N(A)(F_n) = N(A^*)(F_n). \tag{7}$$

Since $(L_n^*) = (L_n)$, it follows from (7) that

$$(L_n)^2 = 5(F_n).$$

The sum, taken termwise, of (A_n) and (A_n^*) is $A_0(L_n)$. Of course, $((A_n^*)^*) = (A_n)$. Several identities involving (A_n) and its dual can be derived as special cases of general identities in [5]; among them are the following, which are generalizations of well known identities for (F_n) and (L_n).

$$A_nA_n^* + N(A)F_n^2 = (-1)^nA_0^2 ,$$

$$F_{2n}A_0 = F_n(A_n + A_n^*) = A_0F_nL_n .$$

Using the theory of binary quadratic forms, it may be shown that distinct recurrences of norm m (where distinct recurrences are recurrences which are not translates or scalar multiples of each other) are in a one-one correspondence with roots n of

$$n^2 \equiv 5 \pmod{4m} ,$$

where $0 \leqslant n < 2m$. It follows that there are recurrences with norm m if and only if $(p/5) = 0$ or 1 for all prime factors p of m, and that the number of distinct recurrences of norm m is 2^r where r is the number of prime factors p of m such that $(p/5) = 1$ (i.e., $p = 10k \pm 1$). Also, it is not possible for 25 to divide the norm. These results may be found in [2] and [4]. In [1] there is a table of the recurrences having a given norm for all possible norms up to 1000.

We remark that multiplication of recurrences with a given discriminant d ($d = 5$ in this paper) corresponds to the composition of binary quadratic forms of the same discriminant; in fact, (4) and (5) are used in the definition of composition of forms.

The following theorem shows that (A_n^*) is in a sense the inverse of (A_n), since (F_n) is the multiplicative identity.

Theorem 1. $X = (A_n^*)$ is the only recurrence satisfying $(A_n)X = N(A)(F_n)$.

Proof. By setting $C_0 = 0$, $C_1 = N(A)$, $m = n = 0$ in (4) and (5) and solving simultaneously for B_0 and B_1, we find that $B_0 = A_0 = A_0^*$ and $B_1 = A_1 - A_0 = -A_1^*$. Thus, if signs are disregarded, $(B_n) = (A_n^*)$, proving the theorem.

Theorem 2. The dual map is an automorphism of the group of recurrences under multiplication.

Proof. By (7), if $(A_n)(B_n) = (C_n)$ then

$$N(A)N(B)(F_n) = (A_n)(B_n)(A_n^*)(B_n^*) = (C_n^*)((A_n^*)(B_n^*)) ,$$

whence $(A_n^*)(B_n^*) = (C_n^*)$ by Theorem 1. Since the dual map is bijective, the theorem follows.

Theorem 3. Any automorphism of the multiplicative group of recurrences preserves the value of the norm.

Proof. By (7),

$$(A_n)(A_n^*) = N(A)(F_n).$$

Let $(A_n) \to (A_n')$ be an automorphism. Then

$$(A_n')(A_n^{*\prime}) = N(A)(F_n') = N(A)(F_n) ,$$

since an automorphism must map the multiplicative identity onto itself. Thus, by Theorem 1, $(A_n^{*\prime}) = (A_n'^*)$, so that $N(A') = N(A'^*) = N(A^{*\prime})$, and the theorem follows by the multiplicative property of the norm.

Let $S = \{p_1, p_2, \cdots\}$ be a subset of the set Q of primes which are quadratic residues of 5 and let $S' = Q - S$. Then the function T mapping recurrences onto recurrences such that

$$T((A_n)) = \begin{cases} (A_n^*) & \text{if } N(A) \in S \\ (A_n) & \text{if } N(A) \in S' \end{cases}$$

determines an automorphism, and any automorphism of the multiplicative group of recurrences can be so characterized. The proof, which uses Theorem 3 and the Unique Factorization Theorem to be proved later, is left to the reader.

Theorem 4. Consider recurrences (G_n) and (H_n) such that

$$N(G) = m_1^2, \qquad N(H) = m_2^2, \qquad (m_1, m_2) = 1.$$

Then

$$(G_n)(H_n) = m_1m_2(F_n)$$

if and only if

$$(G_n) = m_1(F_n) \qquad \text{and} \qquad (H_n) = m_2(F_n).$$

Proof. Suppose $m_1m_2(F_n)=(G_n)(H_n)$. Multiplying by (G_n^*),

$$m_1m_2(G_n^*) = (G_n)(G_n^*)(H_n) = m_1^2(H_n) \ .$$

Thus,

$$m_2(G_n^*) = m_1(H_n).$$

It follows that

$$m_2G_i^* = m_1H_i$$

for all i. Since $(m_1, m_2) = 1$, then $m_1 \mid G_i^*$ and $m_2 \mid H_i$. Therefore,

$$m_2(G_n^*) = m_1(H_n) = m_1m_2(E_n)$$

for some recurrence (E_n), whence

$$m_1^2 = N(G) = N(G^*) = N(m_1E) = m_1^2N(E) \ ,$$

so that $N(E) = 1$. It has been shown in [2] that there is only one recurrence whose norm is 1: namely (F_n). Hence, $(E_n) = (F_n)$.

The converse is obvious.

Theorem 5. (Unique Facorization). Recurrences of a given norm whose terms have no common divisor factor uniquely up to order and sign into recurrences whose norms are the prime divisors of m.

Proof. First we shall show that a recurrence (E_n) can be factored uniquely into recurrences whose norms are (relatively prime) maximal prime power divisors of m. It is only necessary to prove uniqueness for $m = m_1m_2$ with $(m_1,m_2) = 1$, and uniqueness for prime power divisors follows.

If $N(E)$ has only one prime power factor or if $(E_n) = (F_n)$, we are done. Otherwise, let (E_n) have at least two relatively prime factors m_1 and m_2, and assume that factorization is unique for recurrences whose norms are those relatively prime factors. We shall show that (E_n) factors uniquely.

Since there are 2^r recurrences with norm m_1,, where r is the number of prime divisors p of m_1 satisfying $(p/5) = 1$ and assuming that $(p/5) = -1$ for no divisors of m_1 (see [2]), and since, under similar conditions, there are 2^s recurrences with norm m_2, then the set of recurrences obtained by taking products of recurrences, one with each norm is contained in the set of 2^{r+s} recurrences of norm m_1m_2, with equality of sets if and only if any pair of products is distinct. Thus, we must show that if $(A_n)(B_n) = (C_n)(D_n)$ with

$$N(A) = N(C) = m_1, \qquad N(B) = N(D) = m_2, \qquad (m_1,m_2) = 1,$$

then $(A_n) = (C_n)$, $(B_n) = (D_n)$.

Under the conditions stated, there exists a recurrence (G_n), equal to $(A_n^*)(C_n)$ such that $N(G) = m_1^2$ and

$$(A_n)(G_n) = m_1(C_n).$$

Likewise, there is an (H_n) such that

$$N(H) = m_2^2 \qquad \text{and} \qquad (B_n)(H_n) = m_2(D_n).$$

Substituting these relations into

$$(A_n)(B_n) = (C_n)(D_n)$$

we get

$$m_1m_2(A_n)(B_n) = (A_n)(G_n)(B_n)(H_n) \ ,$$

and multiplying by $(A_n^*)(B_n^*)$ and applying (7) obtain

$$m_1m_2(F_n) = (G_n)(H_n).$$

Since $(m_1,m_2) = 1$, we have that $(G_n) = m_1(F_n)$ and $(H_n) = m_2(F_n)$ by Theorem 4. Thus,

$$m_1(C_n) = (A_n)(G_n) = m_1(A_n),$$

whence $(A_n) = (C_n)$, and $(B_n) = (D_n)$, likewise.

Next we show that each of the two recurrences of prime power norm p^k factors uniquely into k recurrences of norm p. Let (A_n) be a recurrence of norm p. Then the only other recurrence of the same norm is (A_n^*) and

no recurrence (except the identity recurrence (F_n)) has a norm dividing p. We shall proceed by induction.

For $k = 1$, the theorem is obviously true. Assume truth for all exponents not greater than k. Then there are two recurrences of norm p^k which factor uniquely, and since $(A_n)^k$ and $(A_n^*)^k$ are factorizations of the recurrences of norm p^k, they are unique factorizations. Multiplying $(A_n)^k$ and $(A_n^*)^k$ by each of the recurrences of norm p and using (7), we get the products

$$(A_n)^{k+1}, \qquad (A_n^*)^{k+1}, \qquad (A_n)^k(A_n^*) = N(A)(A_n)^{k-1}, \qquad \text{and} \qquad (A_n^*)^k(A_n) = N(A)(A_n^*)^{k-1},$$

and the last two products fail to satisfy the requirement that the terms have no common factor. Thus, $(A_n)^{k+1}$ and $(A_n^*)^{k+1}$ are two factorizations of recurrences of norm p^{k+1}, and they are the only two meeting the requirement that the terms of the product have no common factor. Since there are two recurrences of norm p^{k+1} (see [2]), $(A_n)^{k+1}$ and $(A_n^*)^{k+1}$ must be their factorizations. This completes the proof.

REFERENCES

1. Brother U. Alfred, "On the Ordering of Fibonacci Sequences," *The Fibonacci Quarterly,* Vol. 1, No. 4 (December, 1963), pp. 43–46.
2. T.W. Cusick, "On a Certain Integer Associated with a Generalized Fibonacci Sequence," *The Fibonacci Quarterly,* Vol. 6, No. 2 (April, 1968), pp. 117–126.
3. P. Naor, "Letter to the Editor," *The Fibonacci Quarterly,* Vol. 3, No. 4 (December, 1965), pp. 71–73.
4. Dmitri Thoro, "An Application of Unimodular Transformations," *The Fibonacci Quarterly,* Vol. 2, No. 4 (December, 1964), pp. 291–295.
5. Oswald Wyler, "On Second-Order Recurrences," *American Math. Monthly,* 72 (1965) pp. 500–506.

****

A NOTE ON FERMAT'S LAST THEOREM

DAVID ZEITLIN
Minneapolis, Minnesota

In this note, $n, m, x, y,$ and z are all positive integers, with $x < y < z$.

Theorem 1. For $n \geq 2$, the equation $x^n + y^n = z^n$ has no solutions whenever $x + ny \leq nz$.

Corollary. For $m \geq 1$ and $n \geq 2$, $x^{mn} + y^{mn} = z^{mn}$ has no solutions whenever $x^m + ny^m \leq nz^m$.

Proof. Suppose $x^n + y^n = z^n$ has a solution with $y = x + a$, $z = x + b$, where $b > a > 0$ are integers. Then, by using the binomial theorem, we have

$$x^n = z^n - y^n = (x+b)^n - (x+a)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i}(b^i - a^i) = nx^{n-1}(b-a) + Q(n,x,b,a), \quad Q > 0.$$

Thus

$$x^{n-1}(x - n(b-a)) = Q,$$

and so $x - n(b-a) > 0$ is a necessary condition for a solution. Since

$$b - a = (x+b) - (x+a) = z - y, \quad x - n(z-y) \leq 0$$

is the stated result.

REMARKS. Since $nz < ny + x$ is a necessary condition for a solution and since $y < z$, we see that

[Continued on Page 402.]