STRONG DIVISIBILITY SEQUENCES AND SOME CONJECTURES

CLARK KIMBERLING
University of Evansville, Evansville, IN 47702

1. INTRODUCTION

Which recurrent sequences $\{t_n : n = 0, 1, \ldots\}$ satisfy the following equation for greatest common divisors:

(1) $$(t_m, t_n) = t_{(m,n)} \quad \text{for all } m,\ n \geq 1,$$

or the weaker divisibility property:

(2) $$t_m | t_n \quad \text{whenever} \quad m | n?$$

In case the sequence $\{t_n\}$ is a *linear* recurrent sequence, the question leads directly to an unproven conjecture of Morgan Ward. (See [3] for further discussion of this question.) Nevertheless, certain examples have been studied in detail. If t_n is the nth Fibonacci number F_n, then (1) holds and continues to hold if t_n is generalized to the Fibonacci polynomial $F_n(x,z)$, as defined in Hoggatt and Long [2]. Not only does (1) hold for these second-order linear recurrent sequences, but (1) holds also for certain higher-order linear sequences and certain nonlinear sequences. For example, if $\{s_n\}$ and $\{t_n\}$ are sequences of nonnegative integers satisfying (1), then for fixed $m \geq 2$ the sequences $\{t_n^m : n = 0, 1, \ldots\}$ and $\{t_{s_n} : n = 0, 1, \ldots\}$ also satisfy (1). Other examples include Vandermonde sequences, resultant sequences and their divisors, and elliptic divisibility sequences. These are discussed below in Sections 3 and 4, in connection with the main theorem (Theorem 1) of this note.

In the sequel, the term *sequence* always refers to a sequence t_0, t_1, t_2, ... of integers or polynomials (in some finite number of indeterminates) all of whose coefficients are integers. With this understanding, a sequence is a *divisibility sequence* if (2) holds, and a *strong divisibility sequence* if (1) holds. Here, all divisibilities refer to the arithmetic in the appropriate ring; that is, the ring I of integers if $t_n \in I$ for all n, and the ring $I[x_1, \ldots, x_j]$ if the t_n are polynomials in the indeterminates $x_1, \ldots, x_j$.

A sequence $\{t_n\}$ in I (or $I[x_1, \ldots, x_j]$) is a kth-*order linear recurrent sequence* if

(3) $$t_{n+k} = a_1 t_{n+k-1} + \cdots + a_k t_n \qquad n = 0, 1, \ldots,$$

where the a_i's and $t_0, \ldots, t_{n-1}$ lie in I (or $I[x_1, \ldots, x_j]$). A kth-*order divisibility sequence* is a kth-order linear recurrent sequence satisfying (2), and a kth-*order strong divisibility sequence* is a kth-order linear recurrent sequence satisfying (1).

2. CYCLOTOMIC QUOTIENTS

For any sequence $\{t_n\}$ we define *cyclotomic quotients* Q_1, Q_2, ... as follows: for $n \geq 2$, let $P_1, P_2, \ldots, P_r$ be the distinct prime factors of n; let

$$\Pi_0 = t_n,$$

and for $1 \leq k \leq r$, let

$$\Pi_k = \Pi t_{n/P_{i_1} P_{i_2} \ldots P_{i_k}},$$

the product extending over all the k indices i_j which satisfy the conditions

$$1 \leq i_1 < i_2 < \ldots < i_k \leq r.$$

Let $Q_1 = 1$, and for $n \geq 2$, define

$$Q = \frac{\Pi_0 \Pi_2 \cdots}{\Pi_1 \Pi_3 \ldots}. \tag{3}$$

The following lemma is a special case of the inclusion-exclusion principle:

Lemma 1: Let H be a set of τ real numbers. For $i = 1, 2, \ldots, \tau$, let $\mathfrak{H}_i$ be the family of subsets of H which consist of i elements. Let

$$m_i = \sum_{A \in \mathfrak{H}_i} \min A.$$

Then

$$m_1 - m_2 + m_3 - \cdots - (-1)^\tau m_\tau = \max H.$$

Proof: We list the elements of H as $h_1 \leq h_2 \leq \ldots \leq h_\tau = \max H$. Clearly

$$m_i = \binom{\tau - 1}{i - 1} h_1 + \binom{\tau - 2}{i - 1} h_2 + \cdots + \binom{i - 1}{i - 1} h_{\tau - i + 1}$$

for $i = 1, 2, \ldots, \tau$, so that

$$m_1 - m_2 + m_3 - \cdots - (-1)^\tau m_\tau$$

$$= h_1 \sum_{i=0}^{\tau - 1} (-1)^i \binom{\tau - 1}{i} + h_2 \sum_{i=0}^{\tau - 2} (-1)^i \binom{\tau - 2}{i} + \cdots + h_{\tau - 1} \sum_{i=0}^{1} (-1)^i \binom{1}{i} + h_\tau$$

$$= h_\tau.$$

Theorem 1: Let $\{t_n : n = 0, 1, \ldots\}$ be a strong divisibility sequence. Then the product $\Pi_1 \Pi_3 \ldots$ divides the product $\Pi_0 \Pi_2 \ldots$. [That is, the quotients (3) are integers (or polynomials with integer coefficients).]

Proof: Let $n = P_1^{f_1} \ldots P_\nu^{f_\nu}$, and write $t_n = q_1^{h_1} \ldots q_\tau^{h_\tau}$. Then

$$\Pi_0 \Pi_2 \Pi_4 \ldots = t_n \Pi t_{n/P_{i_1} P_{i_2}} \Pi t_{n/P_{i_1} P_{i_2} P_{i_3} P_{i_4}} \ldots, \text{ and} \tag{4}$$

$$\Pi_1 \Pi_3 \Pi_5 \ldots = \Pi t_{n/P_i} \Pi t_{n/P_{i_1} P_{i_2} P_{i_3}} \Pi t_{n/P_{i_1} P_{i_2} P_{i_3} P_{i_4} P_{i_5}} \ldots . \tag{5}$$

Now $t_{n/P_i} = q_1^{h_{i1}} q_2^{h_{i2}} \ldots q_\tau^{h_{i\tau}}$ for $i = 1, 2, \ldots, \nu$, where

$$h_j \geq h_{ij} \text{ for } j = 1, 2, \ldots, \tau, \text{ and } i = 1, 2, \ldots, \nu. \tag{6}$$

Further,

$$t_{n/P_{i_1} P_{i_2}} = \left(t_{n/P_{i_1}}, t_{n/P_{i_2}}\right) = \prod_{j=1}^{\tau} q_j^{\min\{h_{i_1 j}, h_{i_2 j}\}},$$

$$t_{n/P_{i_1} P_{i_2} P_{i_3}} = \left(t_{n/P_{i_1} P_{i_2}}, t_{n/P_{i_1} P_{i_3}}, t_{n/P_{i_2} P_{i_3}}\right) = \prod_{j=1}^{\tau} q_j^{\min\{h_{i_1 j}, h_{i_2 j}, h_{i_3 j}\}},$$

and so on. Consider now for any j satisfying $1 \le j \le \tau$ the set

$$H = \left\{h_{1j},\ h_{2j},\ \ldots,\ h_{\nu j}\right\}.$$

For $1 \le i \le \nu$, let $\mathcal{H}_i$ and m_i be as in Lemma 1. Then the exponent of q_i in $\Pi_0\Pi_2 \ldots$ is $h_j + m_2 + m_4 + \cdots$ and the exponent of q_i in $\Pi_1\Pi_3 \ldots$ is $m_1 + m_3 + \cdots$. Consequently, the exponent of q_i in (3) is

$$h_j - \left[m_1 - m_2 + m_3 - \cdots - (-1)^{\tau} m_{\tau}\right].$$

By Lemma 1, this exponent is $h_j - \max H$, which according to (6) is nonnegative.

It is easily seen that Equation (2) would not be sufficient for the conclusion of Theorem 1: define

$$t_n = \begin{cases} n & \text{for } n = 0, 1, 2, 4, 6, 8, \ldots \\ 2 & \text{for } n = 3 \\ 2n & \text{for } n = 5, 7, 9, 11, \ldots \end{cases}$$

Then Equation (2) is satisfied, but, for example, the cyclotomic quotient t_6t_1/t_2t_3 is not an integer.

3. RESULTANT SEQUENCES AND THEIR DIVISORS

Suppose

$$(7) \qquad X(t) = \prod_{i=1}^{p}(t - x_i) = t^p - X_1t^{p-1} + \cdots + (-1)^p X_p$$

and

$$(8) \qquad Y(t) = \prod_{j=1}^{q}(t - y_j) = t^q - Y_1t^{q-1} + \cdots + (-1)^q Y_q$$

are polynomials; here any number of the roots x_i and y_j may be indeterminates, and we assume that the coefficients X_k and Y_ℓ lie in the ring $I[x_1, \ldots, x_p, y_1, \ldots, y_q]$. Thus all roots which are not indeterminates must be algebraic integers. Instead of regarding the roots as given indeterminates, we may regard any number of the coefficients X_k and Y_ℓ as the given indeterminates; in this case the roots x_i and y_j are regarded as indeterminates having functional interdependences.

The *resultant sequence* based on $\{x_1, \ldots, x_p, y_1, \ldots, y_q\}$ (or $\{X_1, \ldots, X_p, Y_1, \ldots, Y_q\}$) is the sequence $\{t_n : n = 0, 1, \ldots\}$ given by

$$(9) \qquad t_n = \prod_{j=1}^{q}\prod_{i=1}^{p}\frac{x_i^n - y_j^n}{x_i - y_j}.$$

Note that $t_n = R_n/R_1$, where R_n is the resultant of the polynomials

$$\prod_{i=1}^{p}(t - x_i^n) \quad \text{and} \quad \prod_{j=1}^{q}(t - y_j^n).$$

By a *divisor-sequence* of a resultant sequence $\{t_n\}$, we mean a linear divisibility sequence $\{s_n : n = 0, 1, \ldots\}$ such that $s_n | t_n$ for $n = 1, 2, \ldots$.

We may now state Ward's conjecture mentioned in Section 1: every linear divisibility sequence is (essentially) a divisor-sequence of a resultant sequence. We further conjecture: every linear *strong* divisibility sequence of *integers* must lie in the class T of second-order sequences (i.e., Fibonacci sequences) or else be a product-sequence $\{t_{1n}t_{2n} \ldots t_{mn} : n = 0, 1, \ldots\}$ where each divisor-sequence $\{t_{jn} : n = 0, 1, \ldots\}$ lies in T, for $j = 1, 2, \ldots, m$. The interested reader may wish to consult especially Theorem 5.1 of Ward [8].

One salient class of divisor-sequences of resultant sequences are the *Vandermonde sequences*, as discussed in [3]. Briefly, a Vandermonde sequence $\{t_n : n = 0, 1, \ldots\}$ arises from the polynomial (7) by

$$t_n = \prod_{1 \le i \le j \le p} \frac{x_i^n - x_j^n}{x_i - x_j}.$$

Thus, t_n is akin to the discriminant of the polynomial

$$\Xi(t) = \prod_{i=1}^{p} (t - x_i^n),$$

as well as the resultant of $\Xi(t)$ and its derivative $\Xi'(t)$. (See, for example, van der Waerden [5, pp. 86-87].)

If one or more of the roots x_i and y_j underlying a divisor-sequence of a resultant sequence is an indeterminate, then, except for certain possible irregularities which need not be mentioned here, the sequence is a strong linear divisibility sequence.

As an example of a strong linear divisibility sequence of polynomials, we mention the 6th-order Vandermonde sequence which arises from

$$X(t) = t^3 - \sqrt[3]{x}t^2 - 1.$$

With generating function

$$\frac{t(t^2 + t + 1)^2}{(t^2 + t + 1)^3 + xt^2(t + 1)^2},$$

this sequence $\{t_n\}$ has, for its first few terms, $t_0 = 0$, $t_1 = 1$, $t_2 = -1$, $t_3 = -x$, $t_4 = 2x + 1$, $t_5 = x^2 + x - 1$, $t_6 = -3x^2 - 8x$, $t_7 = -x^3 - x^2 + 9x + 1$, $t_8 = 4x^3 + 18x^2 + 6x - 1$. If $x = -1$, then $\{t_n\}$ is no longer a *strong* linear divisibility sequence, but is, of course, still a divisibility sequence. As reported in [3], we have

$$|t_n| \le F_n \qquad (= n\text{th Fibonacci number})$$

for $1 \le n \le 100$. It is not yet known if this inequality holds for all n.

Another conjecture follows: for any strong linear divisibility sequence of polynomials $t_0, t_1, t_2, \ldots$ which has no proper divisor-sequences, the polynomial t_n is irreducible if and only if n is a prime. A stronger conjecture is that the cyclotomic quotients (3) are all irreducible polynomials.

4. ELLIPTIC DIVISIBILITY SEQUENCES

Consider the sequence of polynomials in x, y, z defined recursively as follows:

$$t_0 = 0,\ t_1 = 1,\ t_2 = x,\ t_3 = y,\ t_4 = xz,$$

$$t_{2n+1} = t_{n+2}t_n - t_{n-1}t_{n+1} \qquad \text{for } n \ge 2$$

$$t_{2n+2} = \frac{1}{x}(t_{n+3}t_{n+1}t_n - t_{n+1}t_{n-1}t_{n+2}) \qquad \text{for } n \ge 2.$$

The sequence $\{t_n : n = 0, 1, \ldots\}$ is an *elliptic divisibility sequence*. If x, y, or z is an indeterminate then $\{t_n\}$ is a strong divisibility sequence. In this case, we conjecture, as in Section 3 for linear sequences, that the cyclotomic quotients (3) are the irreducible divisors of the polynomials t_n.

If x, y, and z are all integers, then $\{t_n\}$ is a strong divisibility sequence if and only if the greatest common divisor of y and xz is 1, as proved in [11].

We conclude with a list of the first several terms of a numerical elliptic strong divisibility sequence:

$t_0 = 0$
$t_1 = 1$
$t_2 = 1$
$t_3 = -1$
$t_4 = 1$
$t_5 = 2$
$t_6 = -1$
$t_7 = -3$
$t_8 = -5$
$t_9 = 7$
$t_{10} = -4$
$t_{11} = -23$
$t_{12} = 29$
$t_{13} = 59$
$t_{14} = 129$
$t_{15} = -314$
$t_{16} = -65$
$t_{17} = 1529$
$t_{18} = -3689$
$t_{19} = -8209$
$t_{20} = -16264$
$t_{21} = 83313$
$t_{22} = 113689$
$t_{23} = -620297$
$t_{24} = 2382785$
$t_{25} = 7869898$
$t_{26} = 7001471$
$t_{27} = -126742987$
$t_{28} = -398035821$
$t_{29} = 1687054711$
$t_{30} = -7911171596$.

REFERENCES

1. Marshall Hall, "Divisibility Sequences of Third Order," *Amer. J. Math.* 58 (1936):577-584.
2. V. E. Hoggatt, Jr., & C. T. Long, "Divisibility Properties of Generalized Fibonacci Polynomials," *The Fibonacci Quarterly* 2, No. 2 (1974):113-120.
3. Clark Kimberling, "Generating Functions of Linear Divisibility Sequences," *The Fibonacci Quarterly* (to appear).
4. Clark Kimberling, "Strong Divisibility Sequences with Nonzero Initial Term," *The Fibonacci Quarterly* 16, No. 6 (1978):541-544.
5. B. L. van der Waerden, *Modern Algebra* (New York: Ungar, 1953).
6. Morgan Ward, "Note on Divisibility Sequences," *Bull. AMS* 42 (1936):843-845.
7. Morgan Ward, "Linear Divisibility Sequences," *Transactions AMS* 41 (1937):276-286.
8. Morgan Ward, "Arithmetical Properties of Sequences in Rings," *Annals of Math.* 39 (1938):210-219.
9. Morgan Ward, "A Note on Divisibility Sequences," *Bull. AMS* 45 (1939):334-336.
10. Morgan Ward, "The Law of Apparition of Primes in a Lucasian Sequence," *Transactions AMS* 44 (1948):68-86.
11. Morgan Ward, "Memoir on Elliptic Divisibility Sequences," *Amer. J. Math.* 70 (1948):31-74.
12. Morgan Ward, "The Law of Repetition of Primes in an Elliptic Divisibility Sequence," *Duke Math. J.* 15 (1948):941-946.

*****