Lucas sequences and divisibility sequences.

Peter Bala, May 2016

The Lucas sequence of the first kind $U_n \equiv U_n(P, Q)$ is a divisibility sequence: if n divides m then U_n divides U_m. The Lucas sequence of the second kind $V_n \equiv V_n(P, Q)$ is an odd divisibility sequence: if n divides m and m/n is odd then V_n divides V_m. We give some examples of linear combinations of Lucas sequences that are either divisibility sequences or odd divisibility sequences.

1. Introduction. One of the many arithmetical properties of the sequence of Fibonacci numbers $F(n)$ is that it is a divisibility sequence: $F(n)$ divides $F(m)$ whenever n divide m. The companion sequence of Lucas numbers $L(n)$ is not a divisibility sequence. However, it does have the weaker property that if n divides m and m/n is odd then $L(n)$ divides $L(m)$. We shall refer to sequences having this property as *odd divisibility sequences*. Somewhat surprisingly, certain linear combinations of Fibonacci numbers or of Lucas numbers also yield divisibility sequences or odd divisibility sequences. For example, the following sequences are all divisibility sequences

$$F(2n) + F(4n)$$

$$F(4n) + F(6n)$$

$$F(6n) + F(8n)$$

$$\dots$$

$$F(3n) - 2F(n) + F(-n)$$

$$F(4n) - 2F(2n)$$

$$F(5n) - 2F(3n) + F(n)$$

$$F(6n) - 2F(4n) + F(2n)$$

$$\dots$$

$$F(4n) - 2F(2n)$$

$$F(8n) - 4F(6n) + 6F(4n) - 4F(2n)$$

$$F(12n) - 6F(10n) + 15F(8n) - 20F(6n) + 15F(4n) - 6F(2n)$$

$$\dots$$

$$L(2n) - L(0)$$

$$L(3n) - L(n)$$

$$L(4n) - L(2n)$$

...

$$L(6n) - 3L(4n) + 3L(2n) - L(0)$$
$$L(7n) - 3L(5n) + 3L(3n) - L(n)$$
$$L(8n) - 3L(6n) + 3L(4n) - L(2n)$$

...

while the following sequences are examples of odd divisibility sequences

$$F(3n) - F(n)$$
$$F(4n) - F(2n)$$
$$F(5n) - F(3n)$$

...

$$F(3n) + 2F(n) + F(-n)$$
$$F(4n) + 2F(2n)$$
$$F(5n) + 2F(3n) + F(n)$$
$$F(6n) + 2F(4n) + F(2n)$$

...

$$L(2n) + L(0)$$
$$L(3n) + L(n)$$
$$L(4n) + L(2n)$$

...

$$L(4n) \pm 2L(2n) + L(0)$$
$$L(5n) \pm 2L(3n) + L(n)$$
$$L(6n) \pm 2L(4n) + L(2n)$$

...

The method of proof of these assertions is the same in each case and, as might be expected, can be applied to more general Lucas sequences. Let us recall the definition and some of the basic properties of Lucas sequences.

2. Lucas sequences.

Let P, Q be nonzero integers, and let α, β be the two complex zeros of the quadratic polynomial $x^2 - Px + Q$:

$$\alpha = \frac{P + \sqrt{P^2 - 4Q}}{2}$$

$$\beta = \frac{P - \sqrt{P^2 - 4Q}}{2}$$

with

$$\alpha + \beta = P, \qquad \alpha\beta = Q.$$

We suppose α and β are distinct, that is, $P^2 \neq 4Q$.

The Lucas sequences of the first and second kind, denoted by $U_n(P, Q)$ and $V_n(P, Q)$ respectively, are integer sequences defined by

$$U_n \equiv U_n(P, Q) = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \qquad V_n \equiv V_n(P, Q) = \alpha^n + \beta^n.$$

They both satisfy the same second-order linear recurrence equation but with different initial conditions, namely

$$U_n = PU_{n-1} - QU_{n-2}, \qquad U_0 = 0, U_1 = 1$$

$$V_n = PV_{n-1} - QV_{n-2}, \qquad V_0 = 2, V_1 = P.$$

Lucas sequences of the first kind $U_n(P, Q)$ are divisibility sequences: this follows easily from the fact that $x^n - y^n$ divides $x^{nm} - y^{nm}$ in the ring $\mathbb{Z}[x, y]$, and the observation that the resulting polynomial $(x^{nm} - y^{nm})/(x^n - y^n)$ is symmetric in x and y and so can be written as an integral polynomial in the variables $x + y$ and xy. Lucas sequences of the second kind $V_n(P, Q)$ are odd divisibility sequences: this follows from the observation that the polynomial $x^n + y^n$ divides $x^{nm} + y^{nm}$ in the ring $\mathbb{Z}[x, y]$ provided m is odd.

The Fibonacci and Lucas numbers are examples of Lucas sequences with parameter Q equal to -1,

$$F(n) = U_n(1, -1), \qquad L(n) = V_n(1, -1).$$

The even-indexed Fibonacci and Lucas numbers are examples of Lucas sequences with parameter Q equal to 1,

$$F(2n) = U_n(3, 1), \qquad L(2n) = V_n(3, 1).$$

In Tables 1 through 4 we give some examples of divisibility and odd divisibility sequences formed from linear combinations of Lucas sequences involving the binomial coefficients. Notice in each case the Lucas sequences have the second parameter Q equal to either 1 or -1: r and s are arbitrary integers.

Table 1. $U_n = U_n(P,1), \quad V_n = V_n(P,1)$

Divisibility sequences
U_{rn}
$V_{rn} - V_{(r+s)n}$
$U_{rn} - 2U_{(r+s)n} + U_{(r+2s)n}$
$V_{rn} - 3V_{(r+s)n} + 3V_{(r+2s)n} - V_{(r+3s)n}$
$U_{rn} - 4U_{(r+s)n} + 6U_{(r+2s)n} - 4U_{(r+3s)n} + U_{(r+4s)n}$
...

Table 2. $U_n = U_n(P,1), \quad V_n = V_n(P,1)$

Odd divisibility sequences
U_{rn}
$V_{rn} + V_{(r+s)n}$
$U_{rn} + 2U_{(r+s)n} + U_{(r+2s)n}$
$V_{rn} + 3V_{(r+s)n} + 3V_{(r+2s)n} + V_{(r+3s)n}$
$U_{rn} + 4U_{(r+s)n} + 6U_{(r+2s)n} + 4U_{(r+3s)n} + U_{(r+4s)n}$
...

Table 3. $U_n = U_n(P,-1), \quad V_n = V_n(P,-1)$

Divisibility sequences
U_{rn}
$V_{rn} - V_{(r+2s)n}$
$U_{rn} - 2U_{(r+2s)n} + U_{(r+4s)n}$
$V_{rn} - 3V_{(r+2s)n} + 3V_{(r+4s)n} - V_{(r+6s)n}$
$U_{rn} - 4U_{(r+2s)n} + 6U_{(r+4s)n} - 4U_{(r+6s)n} + U_{(r+8s)n}$
...

Table 4. $U_n = U_n(P,-1), \quad V_n = V_n(P,-1)$

Odd divisibility sequences
U_{rn}
$V_{rn} + V_{(r+2s)n}$
$U_{rn} + 2U_{(r+2s)n} + U_{(r+4s)n}$
$V_{rn} + 3V_{(r+2s)n} + 3V_{(r+4s)n} + V_{(r+6s)n}$
$U_{rn} + 4U_{(r+2s)n} + 6U_{(r+4s)n} + 4U_{(r+6s)n} + U_{(r+8s)n}$
...

We illustrate the common method for proving these results by proving two entries in the tables. Firstly, we consider an entry from Table 1.

Example 1. Let $V_n = V_n(P, 1)$ be a Lucas sequence of the second kind with the parameter $Q = 1$. Let r, s be integers. The sequence $a(n) = V_{rn} - 3V_{(r+s)n} + 3V_{(r+2s)n} - V_{(r+3s)n}$ is a divisibility sequence.

Proof. Without loss of generality we may assume $s > 0$ (since otherwise we can replace r with $r + 3s$ and s with $-s$ in the definition of $a(n)$).

Define the Laurent polynomial

$$\begin{aligned} S_n(x) &= x^{rn} + \frac{1}{x^{rn}} - 3\left(x^{(r+s)n} + \frac{1}{x^{(r+s)n}}\right) + 3\left(x^{(r+2s)n} + \frac{1}{x^{(r+2s)n}}\right) \\ &\quad - \left(x^{(r+3s)n} + \frac{1}{x^{(r+3s)n}}\right), \end{aligned}$$

so that $a(n) = S_n(\alpha)$, where $\alpha = \frac{P+\sqrt{P^2-4}}{2}$.

Therefore

$$\frac{a(nm)}{a(n)} = \frac{S_{nm}(\alpha)}{S_n(\alpha)}.$$

Thus, in order to show that $a(n)$ is a divisibility sequences, we need to show that $S_{nm}(\alpha)/S_n(\alpha)$ is an integer for all positive integers n and m. The idea is to show that $S_{nm}(x)/S_n(x)$ can be expressed as an integral polynomial in the variable $x + 1/x$; if we then specialise $x = \alpha = \frac{P+\sqrt{P^2-4}}{2}$, the result will follow since $\alpha + 1/\alpha = P \in \mathbb{Z}$.

There are two cases to consider according as to whether $2r + 3s$ is positive or negative.

Case 1: Suppose $2r + 3s \geq 0$.

Then we have the factorisation

$$S_n(x) = \frac{(1 - x^{sn})^3 \left(x^{(2r+3s)n} - 1\right)}{x^{(r+3s)n}}.$$

Therefore

$$\frac{S_{nm}(x)}{S_n(x)} = \frac{1}{x^{(r+3s)n(m-1)}} P(x),$$

where

$$\begin{aligned} P(x) &= \frac{\left(1 - x^{snm}\right)^3 \left(x^{(2r+3s)nm} - 1\right)}{\left(1 - x^{sn}\right)^3 \left(x^{(2r+3s)n} - 1\right)} \\ &= x^{(2r+6s)n(m-1)} + \cdots + 1 \end{aligned}$$

is a polynomial in x with integer coefficients, of degree $(2r + 6s)n(m - 1)$.
Hence

$$\frac{S_{nm}(x)}{S_n(x)} = x^{(r+3s)n(m-1)} + \cdots + \frac{1}{x^{(r+3s)n(m-1)}}$$

is a Laurent polynomial with integer coefficients.

By the definition of $S_n(x)$ we see that the left-hand side of the previous equation is invariant under the transformation $x \to 1/x$. It follows that $S_{nm}(x)/S_n(x)$ is an integral linear combination of expressions of the form $x^k + 1/x^k$. Now it is readily shown that the Laurent polynomials $x^k + 1/x^k$ may be expressed as integral polynomials in $x + 1/x$ (either by a simple induction argument or by recalling that $x^k + 1/x^k = T_k(x + 1/x)$, where $T_k(x)$ denotes the Chebyshev polynomial of the first kind). It follows that the Laurent polynomial $S_{nm}(x)/S_n(x)$ can be written as an integral linear combination of powers of $x + 1/x$, as required.

Case 2: Suppose now $2r + 3s < 0$. Since s is positive, r must be negative. As in Case 1 we show $S_{nm}(x)/S_n(x)$ is always an integral polynomial in the variable $x + 1/x$.

This time we write the factorisation of $S_n(x)$ in the form

$$S_n(x) = \frac{\left(1 - x^{sn}\right)^3 \left(1 - x^{|2r+3s|n}\right)}{x^{|r|n}}.$$

Therefore

$$\frac{S_{nm}(x)}{S_n(x)} = \frac{1}{x^{|r|n(m-1)}} P_1(x),$$

where

$$\begin{aligned} P_1(x) &= \frac{\left(1 - x^{snm}\right)^3 \left(1 - x^{|2r+3s|nm}\right)}{\left(1 - x^{sn}\right)^3 \left(1 - x^{|2r+3s|n}\right)} \\ &= x^{2|r|n(m-1)} + \cdots + 1 \end{aligned}$$

is a polynomial in x with integer coefficients, of degree $2|r|n(m - 1)$. Hence

$$\frac{S_{nm}(x)}{S_n(x)} = x^{|r|n(m-1)} + \cdots + \frac{1}{x^{|r|n(m-1)}}$$

is a Laurent polynomial with integer coefficients. The argument can now be completed exactly as in Case 1. □

Here is an example taken from Table 3 involving Lucas sequences with parameter $Q = -1$.

Example 2. Let r, s be integers. Let $V_n = V_n(P, -1)$ be a Lucas sequence of the second kind with the parameter $Q = -1$. The sequence $a(n) = V_{rn} - 3V_{(r+2s)n} + 3V_{(r+4s)n} - V_{(r+6s)n}$ is a divisibility sequence.

Once again there is no loss of generality in assuming $s > 0$. The result when r is even is an immediate consequence of Example 1 on observing that

$$V_{2n}(P, -1) = V_n(P^2 + 2, 1).$$

Suppose now r is odd. We define the Laurent polynomial

$$\begin{aligned} S_n(x) &= x^{rn} + \frac{(-1)^n}{x^{rn}} - 3\left(x^{(r+2s)n} + \frac{(-1)^n}{x^{(r+2s)n}}\right) + 3\left(x^{(r+4s)n} + \frac{(-1)^n}{x^{(r+4s)n}}\right) \\ &\quad - \left(x^{(r+6s)n} + \frac{(-1)^n}{x^{(r+6s)n}}\right), \end{aligned}$$

so that $a(n) = S_n(\alpha)$, where $\alpha = \frac{P+\sqrt{P^2+4}}{2}$. As before, the condition for $a(n)$ to be a divisibility sequence is that $a(nm)/a(n) = S_{nm}(\alpha)/S_n(\alpha)$ is an integer for all positive integers n and m. We will prove this by showing that $S_{nm}(x)/S_n(x)$ is always an integral polynomial in the variable $x - 1/x$; if we then specialise $x = \alpha = \frac{P+\sqrt{P^2+4}}{2}$, the divisibility result will follow since now $\alpha - 1/\alpha = P \in \mathbb{Z}$.

We have the factorization

$$S_n(x) = \frac{\left(1 - x^{2sn}\right)^3 \left(x^{(2r+6s)n} - (-1)^n\right)}{x^{(r+6s)n}}.$$

There are two cases to consider depending on whether $2r + 6s$ is positive or negative. We deal with case $2r + 6s$ is positive. The case when $2r + 6s$ is negative is handled similarly.

We have

$$\frac{S_{nm}(x)}{S_n(x)} = \frac{1}{x^{(r+6s)n(m-1)}} P(x),$$

where

$$P(x) = \frac{\left(1 - x^{2snm}\right)^3 \left(x^{(2r+6s)nm} - (-1)^{nm}\right)}{\left(1 - x^{2sn}\right)^3 \left(x^{(2r+6s)n} - (-1)^n\right)}$$

is readily seen to be a polynomial in $\mathbb{Z}[x]$ for $m = 1, 2, 3, ...,$ of degree $(2r + 12s)n(m - 1)$. Thus $S_{nm}(x)/S_n(x) = x^{(r+6s)n(m-1)} + \cdots + \frac{(-1)^{n(m-1)}}{x^{(r+6s)n(m-1)}}$ is a Laurent polynomial with integer coefficients. We claim $S_{nm}(x)/S_n(x)$ is an integral polynomial in $x - 1/x$. To prove the claim, we will make use of the symmetry properties

$$\frac{S_{nm}(x)}{S_n(x)} = (-1)^{n(m-1)} \frac{S_{nm}\left(\frac{1}{x}\right)}{S_n\left(\frac{1}{x}\right)}$$

and

$$\frac{S_{nm}(x)}{S_n(x)} = (-1)^{n(m-1)} \frac{S_{nm}(-x)}{S_n(-x)}.$$

There are several cases to consider depending on the parity of m and n:

(i) If n is even then $S_{nm}(x)/S_n(x)$ is an even function of x and is symmetric under $x \to 1/x$ and so is an integral linear combination of terms of the form $x^{2k} + 1/x^{2k}$. Therefore, $S_{nm}(x)/S_n(x)$ can be written as an integral linear combination of powers of $x^2 + 1/x^2$, and hence also as an integral linear combination of powers of $x - 1/x$ (since $x^2 + 1/x^2 = (x - 1/x)^2 + 2$).

(ii) If n is odd and m is odd, then again $S_{nm}(x)/S_n(x)$ is an even function of x and is symmetric under $x \to 1/x$, and hence as in part (i), $S_{nm}(x)/S_n(x)$ can be written as an integral linear comination of powers of $x - 1/x$.

(iii) Finally, if n is odd and m is even then $S_{nm}(x)/S_n(x)$ is an odd function of x and changes sign under the transformation $x \to 1/x$, and so is an integral linear combination of terms of the form $x^{2k+1} - 1/x^{2k+1}$, and therefore (for example, by a simple induction argument) is also an integral linear combination of powers of $x - 1/x$. $\square$