A FAMILY OF LINEAR DIVISIBILITY SEQUENCES OF ORDER FOUR

PETER BALA, Feb 2014

A sequence $(a(n))_{n\geq 1}$ of elements of an integral domain D is a divisibility sequence if $a(n)$ divides $a(nm)$ for all n, m and $a(n) \neq 0$. We call $a(n)$ a linear divisibility sequence of order k if the sequence also satisfies a homogeneous linear recurrence of order k with coefficients in D. In [2], Lucas studied a 2-parameter family of second-order divisibility sequences of integers. Lehmer [1] extended the Lucas sequences to a family of fourth-order linear divisibility sequences, dependent on two integer parameters P and Q, with an ordinary generating function (o.g.f.) of the form

$$\frac{z(1+z+Qz^2)}{1-(P-2Q)z^2+Q^2z^4}\,.$$

Williams and Guy [4] found another family of fourth-order linear divisibility sequences, dependent now on three integer parameters P_1, P_2 and Q, having the o.g.f.

$$\frac{z(1-Qz^2)}{1-P_1z+(P_2+2Q)z^2-P_1Qz^3+Q^2z^4}\,.$$

In this note we construct, for each positive odd integer p, a 2-parameter family of fourth-order linear divisibility sequences distinct from those considered by Lehmer and Williams and Guy. The construction depends on the following result.

Proposition 1

Let p be a positive odd integer. The sequence of homogeneous polynomials $\mathrm{P}(n,x,y)$ defined by the formula

$$\mathrm{P}(n,x,y) = (x^n+y^n)(x^{pn}-y^{pn}) \tag{1}$$

is a linear divisibility sequence of order 4 in the integral domain $Z[x,y]$.

Proof

Clearly,

$$\frac{\mathrm{P}(nm,x,y)}{\mathrm{P}(n,x,y)} = \frac{\mathrm{P}(m,X,Y)}{\mathrm{P}(1,X,Y)}\,,$$

where $X = x^n$ and $Y = y^n$. Thus to show that $\mathrm{P}(n,x,y)$ divides $\mathrm{P}(mn,x,y)$ in the ring $\mathrm{Z}[x,y]$ it is sufficient to show that $\mathrm{P}(1,x,y)$ divides $\mathrm{P}(m,x,y)$ in $Z[x,y]$ for every m. We verify this is true on a case-by-case basis by writing $\mathrm{P}(m,x,y)/\mathrm{P}(1,x,y)$ as a product of polynomials in $Z[x,y]$:

Case 1) m is odd: $\mathrm{P}(m,x,y)/\mathrm{P}(1,x,y)$ equals $f(x,y)g(x,y)$, where

$$f(x,y) = \frac{x^m+y^m}{x+y}$$

and

$$g(x,y) = \frac{(x^{pm}-y^{pm})}{(x^p-y^p)}$$

are easily seen to be polynomials in $Z[x,y]$.

Case 2) $m = 2r$ is even with r odd: $\mathrm{P}(m,x,y)/\mathrm{P}(1,x,y)$ equals $f(x,y)g(x,y)h(x,y)$, where

$$f(x,y) = x^m + y^m$$

$$g(x,y) = \frac{(x^{pr} + y^{pr})}{(x+y)}$$

and

$$h(x,y) = \frac{(x^{pr} - y^{pr})}{(x^p - y^p)}$$

are polynomials in $Z[x,y]$.

Case 3) $m = 2r$ is even with r even: $\mathrm{P}(m,x,y)/\mathrm{P}(1,x,y)$ equals $f(x,y)g(x,y)h(x,y)$, where now

$$f(x,y) = x^m + y^m$$

$$g(x,y) = x^{pr} + y^{pr}$$

$$h(x,y) = \frac{(x^{pr} - y^{pr})}{(x+y)(x^p - y^p)}$$

all belong to $Z[x,y]$; here $h(x,y)$ is a polynomial since the polynomials $x + y$ and $x^p - y^p$ are coprime in the UFD domain $Z[x,y]$ for p odd, and both divide $x^{pr} - y^{pr}$ when r is even. Thus $\mathrm{P}(n,x,y)$ is a divisibility sequence.

To see that the sequence $\mathrm{P}(n,x,y)$ obeys a fourth-order linear recurrence we calculate the o.g.f. of the normalized sequence $\mathrm{P}(n,x,y)/\mathrm{P}(1,x,y)$.

From (1), we see that the o.g.f.

$$\sum_{n\geq 1} \frac{\mathrm{P}(n,x,y)}{\mathrm{P}(1,x,y)} z^n,$$

is a sum of four geometric series, and so will be a rational function of the form $z\mathrm{N}(z)/\mathrm{D}(z)$ for polynomials $\mathrm{N}(z)$ and $\mathrm{D}(z)$. A short calculation yields

$$\mathrm{N}(z) = 1 - 2xy\frac{x^p + y^p}{x + y}z + (xy)^{p+1}z^2 \tag{2}$$

$$\mathrm{D}(z) = (1 - x^{p+1}z)(1 - x^p yz)(1 - xy^p z)(1 - y^{p+1}z). \tag{3}$$

From the form of the denominator polynomial $\mathrm{D}(z)$, we see that the normalized sequence $\mathrm{P}(n,x,y)/\mathrm{P}(1,x,y)$, and hence also the sequence $\mathrm{P}(n,x,y)$, satisfies a linear recurrence of order 4, whose coefficients are polynomials in $\mathbb{Z}[x,y]$. $\square$

Integer divisibility sequences

We can use Proposition 1 to get fourth-order linear divisibility sequences of integers by specializing the values of x and y in the polynomials $\mathrm{P}(n, x, y)$, for example, by taking x and y to be distinct integers. However, more is possible as we now show.

Consider the normalized polynomials $\mathrm{A}(n, x, y) := \mathrm{P}(n, x, y)/\mathrm{P}(1, x, y)$. Observe from (1) that for each n, $\mathrm{A}(n, x, y)$ is a symmetric polynomial that is also invariant under change of sign of the variables x and y

$$\mathrm{A}(n, x, y) = \mathrm{A}(n, y, x) = \mathrm{A}(n, -x - y).$$

Clearly, the same symmetries also hold for the polynomial $\mathrm{A}(nm, x, y)/\mathrm{A}(n, x, y)$ for all natural numbers n, m. It is a simple consequence of the fundamental theorem of symmetric polynomials that these polynomials can be written as a polynomials with integer coefficients in the symmetric functions $(x + y)^2$ and xy. Thus in order for $\mathrm{A}(n, x, y)$ to be a divisibility sequence consisting of integers it suffices to choose values for x and y so that both $(x+y)^2$ and xy are integers. Accordingly, let P and Q be nonzero integers and define complex numbers α and β by

$$\begin{aligned} (\alpha + \beta)^2 &= P \\ \alpha\beta &= Q \end{aligned} \tag{4}$$

so that α and β are the roots of the quadratic equation $x^2 - \sqrt{P}x + Q = 0$. We also assume that α/β is not equal to a root of unity. Then

$$\mathrm{A}(n, \alpha, \beta) = \frac{(\alpha^n + \beta^n)(\alpha^{pn} - \beta^{pn})}{(\alpha + \beta)(\alpha^p - \beta^p)} \tag{5}$$

is a well-defined fourth-order linear divisibility sequence of integers.

Example 1 Suppose that $p = 3$. The o.g.f of the sequence $\mathrm{A}(n) \equiv \mathrm{A}(n, \alpha, \beta)$ given by (5) can be calculated from (2) and (3). It is straightforward to express this result in terms of the integer parameters P and Q. We find

$$\sum_{n \geq 1} \mathrm{A}(n) z^n = \frac{z\mathrm{N}(z)}{\mathrm{D}(z)},$$

where

$$\mathrm{N}(z) = z(1 - 2Q(P - 3Q)z + Q^4 z^2) \tag{6}$$

and

$$\begin{aligned} \mathrm{D}(z) &= 1 - P_1 z + (P_2 - 2Q^4)z^2 - P_1 Q^4 z^3 + Q^8 z^4 \\ &= (1 + Q(2Q - P)z + Q^4 z^2)(1 - (P^2 - 4PQ + 2Q^2)z + Q^4 z^2) \end{aligned} \tag{7}$$

where

$$P_1 = P(P - 3Q) \quad \text{and} \quad P_2 = PQ(P^2 - 6PQ + 10Q^2).$$

From (7), we see that $\mathrm{A}(n)$ satisfies the fourth-order linear recurrence

$$A(n) = P_1 A(n-1) - (P_2 - 2Q^4)A(n-2) + P_1 Q^4 A(n-3) - Q^8 A(n-4)\,.$$

Example 1 continued Still with $p = 3$ choose $P = 5$ and $Q = 1$.
Then by (4), $\alpha = (1+\sqrt{5})/2 = \phi$, the golden ratio, and $\beta = 1/\phi$. The sequence $\mathrm{A}(n) \equiv \mathrm{A}(n, \alpha, \beta)$ of (5) is given by the formula

$$\mathrm{A}(n) = \frac{1}{4\sqrt{5}}(\phi^n + \phi^{-n})(\phi^{3n} - \phi^{-3n})$$

with o.g.f. from (6) and (7) equal to

$$\frac{1 - 4z + z^2}{(1 - 3z + z^2)(1 - 7z + z^2)}\,.$$

The first few terms of the sequence are $1, 6, 38, 252, 1705, 11628, 79547, 544824$, ... This is A215466 in the database.

REFERENCES

[1] D. H. Lehmer, An extended theory of Lucas' Functions, Annals of Mathematics Second Series, Vol. 31, No. 3 (July 1930), 419-448.

[2] E. Lucas, Théorie des Fonctions Numériques Simplement Périodiques.

[3] Wikipedia, Lucas sequence

[4] H. C. Williams and R. K. Guy, Some fourth-order linear divisibility sequences, Intl. J. Number Theory 7 (5) (2011) 1255–1277.