Some Extensions of the Lucas Functions

R. K. Guy, Calgary
E. Roettger, Mount Royal
H.C. Williams, Calgary

Lucas' Functions

The Lucas functions u_n and v_n are defined by

$$u_n = u_n(p, q) = (\alpha^n - \beta^n)/(\alpha - \beta),$$

and

$$v_n = v_n(p, q) = \alpha^n + \beta^n,$$

where α and β are the zeros of the polynomial $x^2 - px + q$, and p, q are rational integers and $(p, q) = 1$.

Some Simple Observations

We have $u_0=0, u_1=1,$

$$u_{n+1} = pu_n - qu_{n-1}$$

The sequence $\{u_n\}$ is a divisibility sequence. That is, $u_m \mid u_n$ whenever $m|n$ and $u_m \neq 0$.

For example, the Fibonacci numbers $\{F_n\}$ satisfy $F_{n+2} = F_{n+1} + F_n$ and $F_m|F_n$ whenever $m \mid n$.

Addition Formulas

$$2\, u_{m+n} = v_m u_n + u_m v_n, \quad 2\, v_{m+n} = v_m v_n + \Delta u_m\, u_n$$

Here $\Delta = (\alpha-\beta)^2 = p^2 - 4q$.

When $n=m$, we get the duplication formulas:

$$u_{2n} = u_n v_n, \qquad 2v_{2n} = v_n{}^2 + \Delta u_n{}^2.$$

Note that Lucas' theory involved two functions.

Multiplication Formulas

These are formulas that express u_{mn} and v_{mn} in terms of u_n, v_n and p, q.

We have

$$u_{mn}/u_n = \sum_{i=0}^{[m/2]} C(i)\, q^{ni} \Delta^{[m/2]-i}\, u_n^{m-2i+1}, \quad (m \text{ odd})$$

and

$$v_{mn} = \sum_{i=0}^{[m/2]} C(i)(-1)^i q^{ni}\, v_n^{m-2i},$$

where $C(j) = m(m-j-1)!/(j!(m-2j)!)$.

The Law of Apparition for $\{u_n\}$

Let r be any prime such that $r \nmid 2q$.

If $\varepsilon = (\Delta/r)$, then $r \mid u_{r-\varepsilon}$.

The law of Repetition for $\{u_n\}$

If $r^{\lambda} \| u_n$, then

$$r^{\lambda+\mu} \| u_{nr^{\mu}} \quad \text{if } r^{\lambda} \neq 2,$$
$$r^{\lambda+\mu} \mid u_{nr^{\mu}} \quad \text{if } r^{\lambda} = 2.$$

Lucas (Théorie des Nombres)

The theory of [linear] recurrent sequences is an inexhaustible mine which contains all the properties of numbers; by calculating the successive terms of such sequences, decomposing them into their prime factors and seeking out by experimentation the laws of apparition and repetition of the prime numbers, one can advance in a systematic manner the study of the properties of numbers and their application to all branches of mathematics.

Lucas' Fundamental Theorem

Let N be an odd positive integer and $T = N\text{-}1$ or $N+1$.

<u>Theorem</u> (Lucas). If $N | u_T$ and $N \nmid u_{T/d}$ for all d such that $0<d<t$ and $d|T$, then N is a prime.

<u>Theorem</u> (Lehmer). If $N | u_T$ and $N \nmid u_{T/r}$ for each distinct prime divisor r of T, then N is a prime.

<u>Theorem</u>. If $N | u_T$ and $N | u_T / u_{T/r}$ for each distinct prime divisor r of T, then N is a prime.

Applications

Lucas was particularly interested in how these functions could be employed in proving the primality of certain large integers, and as part of his investigations succeeded in demonstrating that the Mersenne number $2^{127}-1$ is a prime.

This was a most remarkable achievement, and is one of the first important results of what we now call computational number theory. In modern parlance, a problem that formerly required exponential time to solve was solved by Lucas in polynomial time.

Lucas' Ideas 1878

It was Lucas himself who wished to generalize his sequences.

In 1878 he wrote,

"We have further indicated a first generalization of the principal idea of this memoir in the study of recurrence sequences which arise from the symmetric functions of the roots of algebraic equations of the third and fourth degree and, more generally, of the roots of equations of any degree with rational coefficients."

Lucas' Ideas 1891

"We believe that, by developing these new methods [concerning higher-order linear recurrence sequences], by searching for the addition and multiplication formulas of the numerical functions which originate from the recurrence sequences of the third or fourth degree, and by studying in a general way the laws of the residues of these functions for prime moduli…, we would arrive at important new properties of prime numbers."

One of Lucas' Approaches

Lucas showed that

$$q^{n-1}u_{m-n}u_{m+n} = u_n^2u_{m-1}u_{m+1} - u_m^2u_{n-1}u_{n+1}$$

$$-\Delta^2 q^{n-1}u_{m-n}u_{m+n} = v_n^2v_{m-1}v_{m+1} - v_m^2v_{n-1}v_{n+1}.$$

If we put $A_n = q^{n(n-1)/2}u_n$, then

$$A_{m-n}A_{m+n} = A_n^2A_{m-1}A_{m+1} - A_m^2A_{n-1}A_{n+1}.$$

Lucas, who was a geometer, saw this in a 1862 publication of Moutard concerning a certain problem involving the Poncelet polygons.

Properties of Moutard's Function

If $A_0 = 0, A_1 = 1$ and the next three terms of this recurrence are certain fixed functions of *a, b, c , then*

- A_n is a symmetric polynomial of degree n^2-1 in

a, b, c

- $A_n \in \mathbb{Z}\ (n > 0)$
- $\{A_n\}$ is a divisibility sequence
- If $a = \pm b$, then $A_n = q^{n(n-1)} u_n(p, q)$, where $p = 2c$, $q = b^2$.

Why was Lucas Unsuccessful?

Lucas believed that solutions of

$$A_{m-n}A_{m+n} = A_n^2 A_{m-1}A_{m+1} - A_m^2 A_{n-1}A_{n+1}$$

would satisfy linear recurrences of order 3 or 4, but except for some rather uninteresting cases this is generally not so. (Ward 1948)

Fundamental Properties of Lucas' Functions

1. There are two functions of an integer parameter n (v_n and u_n);

2. Both functions are integer valued for $n>0$ and both satisfy linear recurrences (of order two);

3. One of the functions produces a divisibility sequence;

4. There are addition formulas;

5. There are multiplication formulas.

Divisibility Sequences

A sequence $\{A_n\} \subseteq \mathbb{Z}$ $(n>0)$ is said to be a *linear divisibility sequence of order j* if $\{A_n\}$ satisfies a linear recurrence

$$A_{n+j}=c_1 A_{n+j-1}+c_2 A_{n+j-2}+\dots+c_j A_n, \qquad \{c_i\} \subseteq \mathbb{Z},$$

and $A_m \mid A_n$ whenever $m \mid n$ and $A_m \neq 0$.

We usually put $A_0=0$ and we may assume that $A_1=1$.

Linear Divisibility Sequences of order Three

<u>Conjecture</u> (Hall, 1936)

The only linear divisibility sequences of order three are:

$A_n = n^2 a^{n-1}$, $A_n = n u_n(p, q)$, $A_n = u_n(p, q)^2$,

where a is a rational integer or (Ward 1955) there are only a finite number of prime divisors of $\{A_n\}$.

A Theorem

Theorem (Bézivin, Pettö and van der Poorten)
If $\{A_n\}$ is a linear divisibility sequence, then there is a linear recurrence sequence $\{B_n\}$ and a non negative integer r such that

$$B_n = n^r \prod (\alpha_i^n - \beta_i^n)/(\alpha_i - \beta_i),$$

and $A_n | B_n$ for $n=1,2,3\ldots$. Here α_i, β_i $(i=1,2,3\ldots)$ are algebraic numbers.

An Observation

If we put $r=0$, and $\gamma_i=\alpha_i/\beta_i$ $(i=1,2,\ldots,k)$, $\lambda= \beta_1 \beta_2 \ldots \beta_k$, we have

$$B_n= \lambda^{n-1}\prod(\gamma_i^n-1)/(\gamma_i-1),$$

where γ_i $(i=1,2,\ldots,k)$ and λ are algebraic numbers.

Pierce Functions

In an early attempt to find functions with properties similar to those of u_n and v_n, Pierce (1916) considered

$$\Delta_n = \Pi(1-\gamma_i^n), \quad S_n = \Pi(1+\gamma_i^n),$$

where the products are taken over the zeros γ_i $(i=1,\ldots,k)$ of a polynomial of degree k with rational integral coefficients.

Unfortunately, we cannot get u_n from Δ_n

An Extension

We can extend Pierce's idea to produce the functions

$$U_n=\lambda^{n-1}\,\Pi(1-\gamma_i^{\,n})/(1-\gamma_i), \quad V_n=\lambda^n\,\Pi(1+\gamma_i^{\,n}),$$

where λ, γ_i $(i=1,\ldots,k)$ are simply algebraic numbers selected such that the sequence $\{U_n\}$ is constrained to be a linear divisibility sequence.

A Diophantine Problem

What constraints on λ, γ_i $(i=1,\ldots,k)$ are necessary and sufficient for $\{U_n\}$ to be a linear divisibility sequence?

Put $$Q=\lambda^2\gamma_1\gamma_2\ldots\gamma_k,$$

$$\mu_i=\gamma_i+1/\gamma_i, \qquad \kappa_i=e_i(\mu_1,\mu_2,\ldots,\mu_k) \qquad (i=1,2,\ldots,k),$$

where e_i is the *ith* elementary symmetric function of k variables.

Theorem. If $V_1, Q, Q\kappa_i$ $(i=1,2,\ldots,k)$ are all integers, then U_n, V_n are integers for all $n>0$ and $\{U_n\}$ is a divisibility sequence.

The Case of $k=1$

If we put

$p=\lambda(\gamma_1+1)$, $q=\lambda^2\gamma_1$,

we find that p and q must be rational integers and

$U_n=u_n(p,q)$, $V_n = v_n(p,q)$.

Here $\alpha= \lambda$, $\beta= \lambda\gamma_1$.

The Case of k =2

Here we put

$\rho_1 = \lambda(\gamma_1 + \gamma_2)$, $\rho_2 = \lambda(1 + \gamma_1\gamma_2)$, $Q = \lambda^2 \gamma_1\gamma_2$.

We must have Q a rational integer; ρ_1, ρ_2 the zeros of $x^2 - P_1x + P_2$, where P_1 and P_2 are rational integers; and

$U_n = (\alpha_1^n + \beta_1^n - \alpha_2^n - \beta_2^n)/(\alpha_1 + \beta_1 - \alpha_2 - \beta_2)$,

$V_n = \alpha_1^n + \beta_1^n + \alpha_2^n + \beta_2^n$,

where α_i, β_i are the zeros of $x^2 - \rho_i x + Q$ for $i=1,2$.

Here both $\{U_n\}$ and $\{V_n\}$ satisfy

$$X_{n+4} = P_1 X_{n+3} - (P_2 + 2Q) X_{n+2} + P_1 Q X_{n+1} - Q^2 X_n.$$

These $\{U_n\}$ and $\{V_n\}$ sequences are discussed in W. and Guy (2011).

They possess the 5 basic properties of Lucas functions. There is also a law of apparition, a law of repetition and a Fundamental Theorem.

The Case of k=3

In this case we put

$\rho_1=\lambda(\gamma_1+\gamma_2\gamma_3)$, $\rho_2=\lambda(\gamma_2+\gamma_1\gamma_3)$, $\rho_3=\lambda(\gamma_3+\gamma_1\gamma_2)$, $\rho_4=\lambda(1+\gamma_1\gamma_2\gamma_3)$, $Q=\lambda^2\gamma_1\gamma_2\gamma_3$.

We must have Q a rational integer and $\rho_1, \rho_2, \rho_3, \rho_4$ the zeros of

$$x^4-P_1x^3+P_2x^2-P_3x+P_4,$$

where P_1, P_2, P_3, P_4 are rational integers.

Expressions for U_n and V_n

Here we have

$$U_n = (\alpha_1{}^n - \beta_1{}^n + \alpha_2{}^n - \beta_2{}^n + \alpha_3{}^n - \beta_3{}^n + \alpha_4{}^n - \beta_4{}^n)/$$
$$(\alpha_1 - \beta_1 + \alpha_2 - \beta_2 + \alpha_3 - \beta_3 + \alpha_4 - \beta_4),$$

$$V_n = \alpha_1{}^n + \beta_1{}^n + \alpha_2{}^n + \beta_2{}^n + \alpha_3{}^n + \beta_3{}^n + \alpha_4{}^n + \beta_4{}^n,$$

where α_i, β_i are the zeros of $x^2 - \rho_i x + Q$ for $i=1,2,3,4$.

Conditions that $\{U_n\}$ be a Divisibility Sequence

In order for $\{U_n\}$ to be a divisibility sequence, it is necessary and sufficient that $P_1|P_3$ and that

$$P_4=(P_3/P_1)^2+8Q(P_3/P_1)+QP_1^{\,2}-4P_2Q.$$

Here both $\{U_n\}$ and $\{V_n\}$ satisfy

$$X_{n+8}=P_1X_{n+7}-(P_2+4Q)\,X_{n+6}+(P_3+3QP_1)\,X_{n+5}-$$

$$(P_4+2QP_2+6Q^2)X_{n+4}+Q(P_3+3QP_1)\,X_{n+3}-Q^2\,(P_2+4Q)\,X_{n+2}$$

$$+Q^3P_1X_{n+1}-Q^4X_n\,.$$

In fact, if we put

$R_1=P_3/P_1+2Q$, $R_2=P_2-2P_3/P_1-4Q$,
$R_3=P_1^{\ 2}-2P_2-8Q$,

then $Q\,\gamma_i$, $Q/\,\gamma_i\,(i=1,2,3)$ must be the six zeros of

$$x^6-R_1x^5+(3QR_1+R_2)Qx^4-Q^2\,(R_3+2R_1)x^3$$
$$+Q^3(3QR_1+R_2)x^2-Q^4R_1x+Q^6.$$

An Example

If we put $Q=1$, $P_1=56$, $P_2=668$, $P_3=56(44)=2464$, and $P_4=44^2+8(44)+56^2-4(668)=2752$,

we get $\{U_n\}=$
$0, 1, 56, 2415, 100352, 4140081, 170537640, 7022359583, 289143013376, 11905151192865, 490179860527896$ …

This is OEIS A003696, the number of spanning trees in $P_4 \times P_n$.

The Law of Apparition

Here we put

$\Delta = (\alpha_1 - \beta_1 + \alpha_2 - \beta_2 + \alpha_3 - \beta_3 + \alpha_4 - \beta_4)^2 = P_1^2 - 4P_2 + 8P_3/P_1$.

Let $g(x) = x^3 - R_1x^2 + QR_2x - Q^2R_3$ and let D denote the discriminant of $g(x)$.

Suppose r is a prime such that $r \nmid 2QD$ and put

$\varepsilon = (\Delta/r)$.

If $g(x)$ is irreducible modulo r, put $t = r^3 - \varepsilon$;

otherwise, put $t = r - \varepsilon$. Then $r | U_t$.

A Problem

Unfortunately, there does not seem to be a pair of duplication formulas for U_n and V_n.

These are formulas that express U_{2n} and V_{2n} in terms of U_n, V_n and Q, P_1, P_2, P_3, P_4.

We do have $U_{2n} = U_n V_n$, but we cannot find a formula for V_{2n}.

This means that there can be no multiplication formulas in this case.

Some Divisibility Sequences of order 6

We have seen that $\{U_n\}$ and $\{V_n\}$ satisfy a linear recurrence of degree 8. However, Hall(1933) noted the divisibility sequence $\{A_n\}$: *0,1,1,1,5,1,7,8,5,19,11,23,35,27,…* where

$A_{n+6}=-A_{n+5}+A_{n+4}+3A_{n+3}+A_{n+2}-A_{n+1}-A_n.$

Also, Elkies (unpublished) notes

0,1, 1, 2, 7, 5, 20, 27, 49, 106, 155, 331, 560, 1013, 1917, 3310, 6223, …

Here

$A_{n+6}=-A_{n+5}+2A_{n+4}+5A_{n+3}+2A_{n+2}-A_{n+1}-A_n.$

A special Case of U_n

If we consider the case of $\gamma_1 \gamma_2 \gamma_3 = 1$, we then get

$U_n = (\alpha_1^n - \beta_1^n + \alpha_2^n - \beta_2^n + \alpha_3^n - \beta_3^n)/(\alpha_1 - \beta_1 + \alpha_2 - \beta_2 + \alpha_3 - \beta_3)$,

where $\alpha_i \beta_i = Q$, $\alpha_i = Q\gamma_i$ $(i=1,2,3)$ and Q $(=R^2)$ is the square of a rational integer. Here $\lambda = R$.

In this case α_i, β_i are the zeros of $x^2 - \sigma_i x + R^2$ and σ_i $(i=1,2,3)$ are the zeros of $x^3 - S_1 x^2 + S_2 x + S_3$, where S_1, S_2, S_3, R are rational integers such that

$$S_3 = RS_1^2 - 2RS_2 - 4R^3.$$

Here $\{U_n\}$ is a linear divisibility sequence of order 6.

Indeed, in this case both $\{U_n\}$ and $\{V_n\text{-}2R^n\}$ satisfy

$$X_{n+6}=S_1X_{n+5} -(S_2+3Q)X_{n+4} +(S_3+2QS_1)X_{n+3} -Q(S_2+3Q)X_{n+2}$$

$$+Q^2S_1X_{n+1}-Q^3X_n$$

For Hall's sequence, we have $S_1=-1$, $S_2=-4$, $S_3=5$, $Q=R=1$ and for Elkies' sequence $S_1=-1$, $S_2=-5$, $S_3=7$, $Q=R=1$.

Another Example

Let P', Q', R' be arbitrary integers. If we put

$S_1 = P'Q' - 3R'$, $S_2 = P'^3R' + Q'^3 - 5P'Q'R' + 3R'^3$,
$S_3 = R'(P'^2Q'^2 - 2Q'^3 - 2P'^3R' + 4P'Q'R' - R'^3)$, $Q = R'^2$,

then
$U_n = (\alpha^n - \beta^n)(\beta^n - \gamma^n)(\gamma^n - \alpha^n) / [(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)]$,

where α, β, γ are the zeros of $x^3 - P'x^2 + Q'x - R'$.
This sequence $\{U_n\}$ is discussed in detail by Mueller, Roettger and W.(2009).

Results For the Special Case

In this case we have the duplication formulas

$U_{2n}=(W_n+2R^n)U_n$, $2W_{2n}=W_n^2+\Delta U_n^2-4R^nW_n$,

where we put $W_n=V_n-2R^n$ and $\Delta=S_1^2-4S_2+RS_1-12R^2$.

All of the major results concerning Lucas functions have their analogues for the U_n and W_n functions mentioned above.

This includes the addition and multiplication formulas, the laws of apparition, repetition and Lucas' Fundamental Theorem, when we assume that $gcd(S_1, S_2, S_3, R)=1$.

Law of Repetition

Suppose r is a prime such that r does not divide $6DR$.
Suppose further that $r^{\lambda} || U_n$.

If $r | W_n - 6R^n$, then $r^{\lambda+3\mu} || U_{nr^{\mu}}$;

otherwise, $r^{\lambda+\mu} || U_{nr^{\mu}}$.

Law of Apparition

Let $f(x) = x^3 - S_1x^2 + S_2x - S_3$ and let D denote the discriminant of $f(x)$.

Suppose r is a prime such that $r \nmid 2RD$ and put $\varepsilon = (\Delta/r)$.

If $f(x)$ is irreducible modulo r, put $t = r^2 + \varepsilon r + 1$; otherwise, put $t = r - \varepsilon$. Then $r | U_t$.

Fundamental Theorem

Let N be a positive integer such that $(N,6)=1$. Put

$$T=N^2+N+1 \text{ or } N^2-N+1.$$

Theorem. If $N|U_T$ and $N|U_T/U_{T/r}$ for each distinct prime divisor r of T, then N is a prime.

Another Version

Theorem. Suppose $(N,6)=1$. Put $T=N^2 \pm N+1$, and suppose that $T = 3t$, where t is a rational integer.

If $W_t \equiv -3R^t$ and $\Delta U_t^2 \equiv -27R^{2t} \pmod N$

and N does not divide $U_{3t/q}$ for each distinct prime q which divides t, then N is a prime.

An Application

We let u be any fixed integer and put

$K\ (=K_n)=(u^2+u+1)2^{2n}+(2u+1)2^n+1.$

Let $n \geq 1$ and $L\ (=L_n)=(u^2+u+1)2^n+u$.

Note that $L^2+L+1 = vK$, where $v=u^2+u+1.$

Furthermore, let $q\ (\equiv 1 \pmod 3)$ be a prime such that $L^{(q-1)/3}$ is not $1 \pmod q$.

Define r by $4q=r^2+27s^2$.

A Simple Theorem

<u>Theorem</u>

Suppose

$$K(=K_n)=(u^2+u+1)2^{2n}+(2u+1)2^n+1.$$

If $2^n>u^2+3|u|+3$ and S is selected such that $(K/S)=-1$, then K is a prime if and only if

$$S^{(K-1)/2} \equiv -1 \pmod{K}.$$

A Primality Theorem

<u>Theorem.</u> Let $u(\neq -1)$ be a fixed odd integer and suppose that

$$K(=K_n)=(u^2+u+1)2^{2n}+(2u+1)2^n+1$$

is prime. If we put $S_1=-3qr$, $S_2=-27q^3+3r^2q^2$, $R=rq$,

then $L=(u^2+u+1)2^n+u$ is a prime if and only if

$(U_v,L)=1$, $W_t\equiv -3R^t$ and $\Delta U_t^2\equiv -27R^{2t}\ (mod\ L)$, where

$3t=L^2+L+1.$

Examples

K_n and L_n are both prime for

$u=237, \quad n=407$

$u=-257, \quad n=417$

$u=-407, \quad n=533$

$u=289, \quad n=819$

Conclusion

- Lucas was correct about the existence of fourth order analogues of his functions.
- He seems to have been wrong about third order analogues.
- However, there exist sixth order analogues in which the zeros of a cubic polynomial play an important role.
- There likely exist further analogues for $k>3$, but probably more than 2 functions would be required.

Question

Can we characterize all of the linear divisibility sequences of order 4 or 6 or 8?

Note that for any s

$$u_{n+6}=pu_{n+5} -(q-s)u_{n+4}-psu_{n+3}-q(q-s)u_{n+2} +q^2pu_{n+1}-q^3u_n$$