A Look at Some Divisibility Sequences

Eric Roettger
Joint work with: Richard Guy and Hugh Williams

Mount Royal University

eroettger@mtroyal.ca

December 2012

Motivation

Divisibility Sequence

A divisibility sequence is an integer sequence $\{a_n\}$ such that for all natural numbers m, n, if $m \mid n$, then $a_m \mid a_n$.

Lucas' Functions

The Lucas functions u_n and v_n are defined by:

$$u_n = (\alpha^n - \beta^n)/(\alpha - \beta), \qquad v_n = \alpha^n + \beta^n,$$

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 $u_0 = 0$ $u_1 = 1$, and $u_{n+1} = pu_n - qu_{n-1}$.
If $n = ms$, then

$$\begin{aligned} u_n(p,q) &= \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{\alpha^{ms} - \beta^{ms}}{\alpha - \beta} \\ &= \frac{\alpha^m - \beta^m}{\alpha - \beta} \frac{\alpha^s - \beta^s}{\alpha^m - \beta^m} = u_m(p,q) u_s(v_m, q^m). \end{aligned}$$

Fibonacci Numbers

If $p = 1$ and $q = -1$, then $u_n(1, -1) = F_n$, where $\{F_n\}$ satisfies $F_0 = 0$, $F_1 = 1$ and $F_{n+1} = F_n + F_{n-1}$ and $F_m \mid F_n$ whenever $m \mid n$.

Addition Formulas

$2u_{n+m} = u_n v_m + u_m v_n$ and $2v_{n+m} = v_n v_m + \Delta u_n u_m$
Here $\Delta = (\alpha - \beta)^2 = p^2 - 4q$. When $n = m$, we get the duplication formulas: $u_{2n} = u_n v_n$ and $2V_{2n} = v_n^2 + \Delta u_n^2$.

Multiplication Formulas

$$u_{mn} = u_n \sum_{k=0}^{m/2-1} (-1)^k \binom{m-k-1}{k} q^{nk} v_n^{m-2k-1} \qquad (m \text{ even}),$$

$$u_{mn} = u_n \sum_{k=0}^{\lfloor m/2 \rfloor} \frac{m}{k} \binom{m-k-1}{k-1} q^{nk} \Delta^{\lfloor m/2 \rfloor - k} u_n^{m-2k-1} \qquad (m \text{ odd}),$$

$$v_{mn} = \sum_{k=0}^{\lfloor m/2 \rfloor} (-1)^k \frac{m}{k} \binom{m-k-1}{k-1} q^{nk} v_n^{m-2k}.$$

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

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

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

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

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

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

Historical Motivation

It was Lucas himself who wished to generalize these sequences. He wrote: "We believe that, by developing these new methods [concering higher-order 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 finds in particular, in the study of the function

$$U_n = \Delta\left(a^n, b^n, c^n, \ldots\right) / \Delta(a, b, c, \ldots)$$

in which a, b, c, ... designate the roots of the equation, and $\Delta(a, b, c, \ldots)$ the *alternating function* of the roots, or the square root of the discriminant of the equation, the generalization of the principal formulas contained in the first part of this work.

Lucas (Théorie des Nombres)

The theory of 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 appearance and reproduction 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.

Fundamental Properties of Lucas' Functions

1. There are two functions (v_n and u_n);
2. Both functions satisfy linear recurrences (of order two);
3. One of the functions produces a divisibility sequences;
4. There are addition formulas;
5. There are multiplication formulas.

A Cubic Generalization of the Lucas' Functions

Let α, β, γ be the zeros of $X^3 - PX^2 + QX - R$, where P, Q, R are integers. Put $\delta = (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)$, then
$\delta^2 = \Delta = Q^2P^2 - 4Q^3 - 4RP^3 + 18PQR - 27R^2$.

$$\delta C_n = \left(\alpha^n\beta^{2n} + \beta^n\gamma^{2n} + \gamma^n\alpha^{2n}\right) - \left(\alpha^{2n}\beta^n + \beta^{2n}\gamma^n + \gamma^{2n}\alpha^n\right)$$

$$\text{or } C_n = \left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)\left(\frac{\beta^n - \gamma^n}{\beta - \gamma}\right)\left(\frac{\gamma^n - \alpha^n}{\gamma - \alpha}\right) \text{ and}$$

$$W_n = \left(\alpha^n\beta^{2n} + \beta^n\gamma^{2n} + \gamma^n\alpha^{2n}\right) + \left(\alpha^{2n}\beta^n + \beta^{2n}\gamma^n + \gamma^{2n}\alpha^n\right).$$

Some Simple Observations

For a fixed m, $\{C_n\}$ and $\{W_n\}$ both satisfy

$$\begin{aligned} X_{n+6m} &= a_1 X_{n+5m} - a_2 X_{n+4m} + a_3 X_{n+3m} - a_4 X_{n+2m} \\ &\quad + a_5 X_{n+m} - a_6 X_n, \end{aligned}$$

where

$$\begin{aligned} a_1 &= W_m, a_2 = \left(W_m^2 - \Delta C_m^2\right)/4 + R^m W_m, \\ a_3 &= R^m[\left(W_m^2 + \Delta C_m^2\right)/2 + R^{2m}], \\ a_4 &= R^{2m} a_2, a_5 = R^{4m} a_1, a_6 = R^{6m}. \end{aligned}$$

$\{C_n\}$ is a divisibility sequence

Note that if $n = ms$, then

$$C_n(P,Q,R) = \frac{(\alpha^n - \beta^n)(\beta^n - \gamma^n)(\gamma^n - \alpha^n)}{(\alpha-\beta)(\beta-\gamma)(\gamma-\alpha)}$$
$$= \frac{(\alpha^{ms} - \beta^{ms})(\beta^{ms} - \gamma^{ms})(\gamma^{ms} - \alpha^{ms})}{(\alpha-\beta)(\beta-\gamma)(\gamma-\alpha)}$$

$$= \frac{(\alpha^m - \beta^m)(\beta^m - \gamma^m)(\gamma^m - \alpha^m)}{(\alpha-\beta)(\beta-\gamma)(\gamma-\alpha)} \cdot \frac{(\alpha^{ms} - \beta^{ms})(\beta^{ms} - \gamma^{ms})(\gamma^{ms} - \alpha^{ms})}{(\alpha^m - \beta^m)(\beta^m - \gamma^m)(\gamma^m - \alpha^m)}$$
$$= C_m(P,Q,R) \cdot C_s(A_m, B_m, R^m),$$

where $A_n = \alpha^n + \beta^n + \gamma^n$ and $B_n = \alpha^n\beta^n + \beta^n\gamma^n + \gamma^n\alpha^n$ are third order linear recurrences.

Addition Formulas

$$2C_{n+3m} =$$

$$W_m C_{n+2m} + C_m W_{n+2m} - R^m W_m C_{n+m} + R^m C_m W_{n+m} - 2R^{3m} C_n$$

and

$$2W_{n+3m} =$$

$$\Delta C_m C_{n+2m} + W_m W_{n+2m} - R^m W_m W_{n+m} + R^m \Delta C_m C_{n+m} + 2R^{3m} W_n.$$

Multiplication Formulas

$$W_{mn} = \sum \frac{(-1)^{\lambda_0} m(m-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!} R^{n(\lambda_0+\lambda_3)} \tilde{Q}_n^{\lambda_2} v_{\lambda_1-\lambda_2}(\tilde{P}_n, \tilde{Q}_n)$$

and

$$C_{mn}/C_n = \sum \frac{(-1)^{\lambda_0} m(m-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!} R^{n(\lambda_0+\lambda_3)} \tilde{Q}_n^{\lambda_2} u_{\lambda_1-\lambda_2}(\tilde{P}_n, \tilde{Q}_n),$$

where

$$\tilde{P}_n = W_n, \quad \tilde{Q}_n = (W_n^2 - \Delta C_n^2)/4,$$

and the sums are evaluated over all values of λ_0,λ_1, λ_2,λ_3, such that λ_i are non-negative integers that sum to m and $\lambda_1 + 2\lambda_2 + 3\lambda_3 = m$.

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

If we let $\omega(m)$ be the least positive integer n such that $m \mid C_n$, it is not necessarily the case that if $m \mid C_k$, then $\omega(m) \mid k$.

Ranks of Apparition

Let ω_1 be the least positive integer for which $p | C_{\omega_1}$. For $i = 1, 2, \ldots, k$ define ω_{i+1}, if it exists, to be the least positive integer such that $p | C_{\omega_{i+1}}$, $\omega_{i+1} > \omega_i$ and $\omega_j \nmid \omega_{i+1}$ for any $j \leq i + 1$. We define ω_1, ω_2, $\ldots$, ω_k to be the *ranks of apparition for* $\{C_n\}$.

Classification of Primes

(following Adams and Shanks, 1982)

Put $f(x) = x^3 - Px^2 + Qx - R$ and suppose $p \nmid 6R\Delta$.

- p is an *I prime* if $f(x)$ has no zero in $\mathbb{F}_p$
- p is an *Q prime* if $f(x)$ has only one zero in $\mathbb{F}_p$
- p is an *S prime* if $f(x)$ has all three zeros in $\mathbb{F}_p$

Determination

- p is a Q prime if and only if $(\Delta/p) = -1$.
- If $(\Delta/p) = 1$, p is an S prime if and only if

$$u_{\frac{p-1}{3}}(P', Q') \equiv 0 \pmod{p},$$

  where $P' = 2P^3 - 9QP + 27R$, $Q' = (P^2 - 3Q)^3$.
- p is an I prime otherwise.

Some Laws of Apparition

Assume $p \nmid 6R\Delta$.

- If p is an *I prime* there is only one rank of apparition ω of $\{C_n\}$ and $\omega | p^2 + p + 1$.
- If p is a *Q prime* there is only one rank of apparition ω of $\{C_n\}$ and $\omega | p + 1$.
- If p is an *S prime* there can be no more than 3 ranks of apparition of p. If ω is any rank of apparition, we have $\omega | p - 1$.

The Law of Repetition for $\{C_n\}$

Let $p^\lambda || C_n$ $(\lambda \geq 1)$.

- If $p \neq 2$ and $p \nmid W_n - 6R^n$, then

$$p^{\lambda+1} || C_{pn}.$$

- If $p \neq 2$, $p \neq 3$ and $p | W_n - 6R^n$, then

$$p^{\lambda+3} || C_{pn}.$$

- If $p^\lambda = 3$, then $p^{\lambda+3} | C_{3n}$ when $3 | W_n$.
- If $p = 2$, then $2^{\lambda+1} | C_{2n}$.

Some Fourth Order Recurrences, Guy and Williams

Put $f(x) = x^2 - P_1x + P_2$ $(P_1, P_2 \in \mathbb{Z})$ $\Delta = P_1^2 - 4P_2 (\neq 0)$. Let ρ_1, ρ_2 be the zeros of $f(x)$ and let α_i, β_i $(i = 1, 2)$ be the zeros of

$$x^2 - \rho_i x + Q,$$

where $Q \in \mathbb{Z}$ and $(P_1, P_2, Q) = 1$. We define the sequences $\{U_n\}$ and $\{V_n\}$ by

$$U_n = (\alpha_1^n + \beta_1^n - \alpha_2^n - \beta_2^n)/(\rho_1 - \rho_2)$$

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

Recurrence Formulas

For a fixed m $\{U_n\}$ and $\{V_n\}$ both satisfy

$$\begin{aligned} X_{n+4m} &= V_m X_{n+3m} - [2Q^m + (V_m^2 + \Delta U_m^2)/4] X_{n+2m} \\ &\quad + Q^m V_m X_{n+m} - Q^{2m} X_n. \end{aligned}$$

Addition Formulas

$$2U_{m+n} = V_m U_n + U_m V_n - 2Q^n U_{m-n}$$

$$2V_{m+n} V_m V_n + \Delta U_m U_n - 2Q^n V_{m-n}$$

Multiplication Formulas

$$2^m U_{mn} = \sum C(h,i,j,k)(-1)^{k+i} P_1^i 2^{2k+j} V_n^k U_n^{i+j} Q^{nk} u_j(P_1, P_2)$$
$$2^m V_{mn} = \sum C(h,i,j,k)(-1)^{k+i} P_1^i 2^{2k+j} V_n^k U_n^{i+j} Q^{nk} v_j(P_1, P_2)$$

where the sums are taken over all non-negative integers h, i, j, k such that

$$h + i + j + 2k = m$$

and

$$C(h,i,j,k) = m(h+i+j+k-1)!/(h!i!j!k!).$$

The Law of Apparition for $\{U_n\}$ (1)

Note that α_1, α_2, β_1, β_2 are the zeros of

$$F(x) = x^4 - P_1X^3 + (P_2 + 2Q)x^2 - QP_1x + Q^2.$$

The discriminant D of $F(x)$ is given by $D = E\Delta^2Q^2$ where $E = (P_2 + 4Q)^2 - 4QP_1^2$.

The Law of Apparition for $\{U_n\}$ (2)

Let r be a prime such that $r \nmid 2\Delta EQ$.

- If $(\Delta/r) = (E/r) = 1$, there are at most two ranks of apparition of r in $\{U_n\}$ and both divide either $r-1$ or $r+1$.
- If $(\Delta/r) = -1, = (E/r) = 1$, there are at most two ranks of apparition of r in $\{U_n\}$. One divides $r-1$ and the other divides $r+1$. There are exactly two if $r \nmid P_1$.
- If $(\Delta/r) = 1, = (E/r) = -1$, there is only one rank of apparition ω of r in $\{U_n\}$ and $\omega \mid r^2 - 1$. Also, $r^2 \mid U_\omega$.
- If $(\Delta/r) = -1, = (E/r) = -1$, there is only one rank of apparition ω of r in $\{U_n\}$ and $\omega \mid r^2 + 1$. Also, $r^2 \mid U_\omega$.

The Law of Repetition for $\{U_n\}$ (1)

Let $p^\lambda \mid\mid U_n$ Case 1. $p \neq 2$

- If $p \nmid V_n^2 - 16Q^n$, we have $p^{\lambda+\mu} \mid\mid U_{p^\mu n}$
- If $p \mid V_n^2 - 16Q^n$, we have $p^{\lambda+\mu} \mid U_{pn}$
- If $p^{\lambda+2+\nu} \mid\mid U_{pn}$, then $p^{\lambda+\nu+2\mu} \mid\mid U_{p^\mu n}$
- If $p \nmid D$, then $\nu = 0$

The Law of Repetition for $\{U_n\}$ (2)

Case 2. $p = 2$

- If $p^\lambda = 2$, then $p^{\lambda+\mu} \mid U_{p^\mu n}$
- If $\lambda > 1$, then if $2 \mid\mid V_n$, $p^{\lambda+\mu} \mid\mid U_{pn}$
- If $4 \mid V_n$, then $p^{\lambda+2} \mid U_{pn}$
- If $p^{\lambda+2+\nu}$, then $p^{\lambda+\nu+2\mu} \mid\mid U_{p^\mu n}$

Hall and Elkies examples of 6th order Divisibility Sequences

Hall (1933) presented the sequence $\{U_n\}$, where $U_0 = 0,\ U_1 = 1,\ U_2 = 1,\ U_3 = 1,\ U_4 = 5,\ U_5 = 1,\ U_6 = 7,\ U_7 = 8,\ U_8 = 5, \ldots,$ and

$$U_{n+6} = -U_{n+5} + U_{n+4} + 3U_{n+3} + U_{n+2} - U_{n+1} - U_n.$$

Elkies has also developed the sixth order recurrence below (personal communication). For this sequence we have $U_0 = 0,\ U_1 = 1,\ U_2 = 1,\ U_3 = 2,\ U_4 = 7,\ U_5 = 5,\ U_6 = 20,\ U_7 = 27,\ U_8 = 49, \ldots,$ and

$$U_{n+6} = -U_{n+5} + 2U_{n+4} + 5U_{n+3} + 2U_{n+2} - U_{n+1} - U_n.$$

These are not special cases of C_n and yet are divisibility sequences. So what are they?

A Sixth order $\{U_n\}$ and $\{W_n\}$

Let

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

$$W_n = \alpha_1^n + \beta_1^n + \alpha_2^n + \beta_2^n + \alpha_3^n + \beta_3^n.$$

where 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 R, S_1, S_2, S_3 are rational integers such that

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

Some Observations

Here $\{U_n\}$ is a divisibility sequence of order 6.
Indeed, in this case both $\{U_n\}$ and $\{W_n\}$ satisfy

$$\begin{aligned} X_{n+6} &= S_1 X_{n+5} - (S_2 + 3Q)X_{n+4} + (S_3 + 2QS_1)X_{n+3} \\ &\quad -Q(S_2 + 3Q)X_{n+2} + Q^2 S_1 X_{n+1} - Q^3 X_n \end{aligned}$$

where $Q = R^2$. For Hall's sequences, we have $S_1 = -1$, $S_2 = -4$, $S_3 = 5$, $Q = R = 1$ and for Elkies' sequence $S_1 = -1$, $S_2 = -5$, $S_3 = 7$, $Q = R = 1$

A link to something familiar

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

$$S_1 = P'Q' - 3R', \quad S_2 = P'^3R' + Q'^3 - 5P'Q'R' + 3R'^3,$$

$$S_3 = R'(P'^2Q'^2 - 2Q'^3 - 2P'^3R' + 4P'Q'R' - R'^3), \quad Q = R'^2,$$

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 $x^3 - P'x^2 + Q'x - R'$.

Addition Formulas

$$
\begin{aligned}
2W_{2n+m} &= W_nW_{n+m} + \Delta U_{n+m}U_n - R^nW_nW_m \\
&\quad + R^n\Delta U_nU_m + 2R^{n+2m}W_{n-m}, \\
2U_{2n+m} &= W_nU_{n+m} + U_nW_{n+m} - R^nW_nU_m \\
&\quad + R^nU_nW_m - 2R^{n+2m}U_{n-m}.
\end{aligned}
$$

Multiplication Formulas

$$W_{mn} = \sum (-1)^{\lambda_0} \frac{m(m-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!} R^{n(\lambda_0+\lambda_3)} \tilde{Q}_n^{\lambda_2} v_{\lambda_1-\lambda_2},$$

$$U_{mn} = U_n \sum (-1)^{\lambda_0} \frac{m(m-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!} R^{n(\lambda_0+\lambda_3)} \tilde{Q}_n^{\lambda_2} u_{\lambda_1-\lambda_2}.$$

Here the sums are taken over all non-zero integers λ_0, λ_1, λ_2, λ_3 such that

$$\sum_{i=0}^{3} \lambda_i = \sum_{i=0}^{3} i\lambda_i = m$$

and $u_n = u_n(\tilde{P}_n, \tilde{Q}_n)$, $v_n = v_n(\tilde{P}_n, \tilde{Q}_n)$, where $\tilde{P}_n = W_n$, $\tilde{Q}_n = (W_n^2 - \Delta U_n^2)/4$. Note that $\tilde{P}_1 = S_1$, $\tilde{Q}_1 = S_2 - S_1 R + 3R^2$.

The Law of Apparition

Put $\Delta = S_1^2 - 4S_2 + 4S_2 + jRS_1 - 12R^2$. 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 $\epsilon(\Delta/r)$.
If $f(x)$ is irreducible modulo r, put $t = r^2 + \epsilon r + 1$; otherwise, put
$t = r - \epsilon$. Then $r \mid U_t$.

The Law of Repetition

Suppose r is a prime such that $r \nmid 6DR$.
Suppose further that $r^{\lambda} \mid\mid U_n$.

If $r \mid V_n - 4R^n$, then $r^{\lambda+3\mu} \mid\mid U_{nr^{\mu}}$;
otherwise, $r^{\lambda+\mu} \mid\mid U_{nr^{\mu}}$.

The End