Some Primality Tests

Eric Roettger

Mount Royal University
Based on joint work with: Richard Guy and Hugh Williams

eroettger@mtroyal.ca

December 2015

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 $(p, q) = 1$.

A Special Case of the Lucas' Functions

If we let p=1 and q=-1 then $u_n(1,-1) = F_n$ the Fibonacci Numbers, where you can recall

$$F_n : 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$$

and $v_n(1,-1) = L_n$ the Lucas Numbers,

$$L_n : 2, 1, 3, 4, 7, 11, 18, 29, 47, 76, \ldots$$

An Application

Lucas' main interest in them concerned their application to developing primality tests for numbers N of certain forms. These forms can be summarized as

$$N = Ar^n + \gamma, \tag{1}$$

where r is a prime, $r \nmid A$, $\gamma \in \{1, -1\}$ and N is odd.

Special Case

For example, if $A = 1$, $r = 2$ and $\gamma = -1$, then N is the Mersenne number $2^n - 1$.

Lucas' Work

In the 1878 paper *Théorie des fonctions numériques simplement périodiques* Lucas presented three basic tests for N, one when $r = 2$, another for $r = 3$ and a third test when $r = 5$.

We can express his tests in 3 steps

Step 1. Select p, q such that the Jacobi symbol $(\delta/N) = \gamma$.

Step 2. He next defines a sequence $\{s_i\}$, where $s_0 = u_A(p, q)$,

$$s_1 = u_{rA}(p, q) \quad (r = 5) \quad \text{or} \quad s_1 = u_{rA}(p, q)/u_A(p, q) \quad (r = 2, 3)$$

and

$$s_{i+1} \equiv f_r(s_i) \pmod{N} \quad (i \geq 1).$$

Here $f_r(x) \in \mathbb{Z}[x]$ is a polynomial whose degree and coefficients depend on the value of r. For example, he used $f_2(x) = x^2 - 2$, $f_3(x) = x^3 + 3x - 3$ and $f_5(x) = x^5 + 5x^3 + 5x$.

Step 3. The statements of the tests differed slightly for $r = 2$, $r = 3$ and $r = 5$ but in the last case he asserted that N is a prime if the first term of $\{s_i\}$ which is divisible by N is s_n, that N is composite if none of the terms s_0, s_1, s_2, ..., s_n is divisible by N and finally if s_α $(\alpha \leq n)$ is the first term of the sequence that N divides, then the prime divisors of N must have the form $k5^n \pm 1$.

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."

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.

Purpose of this Presentation

1. Introduce two functions (V_n and U_n);
2. Briefly show that these functions provide a higher order recurrence that resembles Lucas' functions;
3. Briefly mention the speed of calculation of these new sequences;
4. Briefly mention a primality test that these new sequences can be employed for.

A Generalization of the Lucas' Functions (Order 4)

Let V_n and U_n be defined by

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

where α_1, β_1, α_2, β_2 are the zeroes of

$$F(x) = x^4 - P_1x^3 + (P_2 + 2Q)x^2 - QP_1x + Q^2,$$

P_1, P_2, $Q \in \mathbb{Z}$, and $(P_1, P_2, Q) = 1$. Also note that, $\alpha_1\beta_1 = \alpha_2\beta_2 = Q$, $\alpha_1 + \beta_1 = \rho_1$, $\alpha_2 + \beta_2 = \rho_2$, where ρ_1, ρ_2 are the zeroes of $x^2 - P_1x + P_2$.

Something interesting

If we put $Q = 0$, then one of α_1, β_1 and one of α_2, β_2 must be zero and

$$V_n = v_n(P_1, P_2), \quad U_n = u_n(P_1, P_2),$$

where $(P_1, P_2) = 1$.

Fourth order linear recurrence

Both $\{V_n\}$ and $\{U_n\}$ satisfy the fourth order linear recurrence

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

Addition Formulas

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

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, $r^2 \mid U_\omega$.

Calculation of $\{U_n\}$ and $\{V_n\}$

We first note that $U_2 = P_1$ and $V_2 = P_1^2 - 2P_2 - 4Q$ and we define for any fixed t

$$K_j = U_{2jt}/2Q^{jt}, \qquad L_j = V_{2jt}/2Q^{jt}.$$

Calculation of $\{U_n\}$ and $\{V_n\}$

$$K_{2j} = 2K_jL_j,$$
$$L_{2j} = L_j^2 + \Delta K_j^2 - 2.$$

$$K_{2j+1} = L_{j+1}K_j + L_jK_{j+1} - K_1,$$
$$L_{2j+1} = L_{j+1}L_J + \Delta K_{j+1}K_j - L_1.$$

Calculation of $\{U_n\}$ and $\{V_n\}$

Let M be any positive integer such that $(Q, M) = 1$ and suppose we wish to compute K_m and $L_m \pmod M$. We let

$$m = \sum_{i=0}^{h} b_{h-i} 2^i$$

be the binary expansion of m, where $b_0 = 1$, $b_i \in \{0, 1\}$ for positive $i \leq h$ and $h = \lceil \log_2 m \rceil$. Let $\mathcal{W}_0$ denote the 4-tuple $\{L_1 \pmod M, K_1 \pmod M, L_2 \pmod M, K_2 \pmod M\}$. We will write this as

$$\mathcal{W}_0 \equiv \{L_1, K_1, L_2, K_2\} \pmod M.$$

Calculation of $\{U_n\}$ and $\{V_n\}$

Suppose $\mathcal{W}_i \equiv \{A, B, C, D\} \pmod{M}$. We define

$$\mathcal{W}_{i+1} \equiv \begin{cases} \{A^2 + \Delta B^2 - 2, 2AB, AC + \Delta BD - L_1, BC + AD - K_1\}, \text{if } b_{i+1} = 0 \\ \{AC + \Delta BD - L_1, BC + AD - K_1, C^2 + \Delta D^2 - 2, 2CD\}, \text{if } b_{i+1} = 1 \end{cases}$$

$\pmod{M}$. By the above formulas we see that

$$\mathcal{W}_h \equiv \{L_m, K_m, L_{m+1}, K_{m+1}\} \pmod{M}.$$

Thus, it requires $7h$ modular multiplications modulo M to compute $V_{2m}/2Q^m$, $U_{2m}/2Q^m \pmod{M}$ when $t = 1$.

Calculation of $\{U_n\}$ and $\{V_n\}$

If we turn our attention to the problem of computing $V_{2mn}/2Q^{mn}$, $U_{2mn}/2Q^{mn} \pmod M$, given $V_{2m}/2Q^m$, $U_{2m}/2Q^m \pmod M$, we see that this can be done just as above with $t = n$.
If, however, we wish to compute $Q^{-(m-1)n}U_{2mn}/U_{2n}$, we first define

$$J_j = Q^{-(j-1)t}U_{2jt}/U_{2t}$$

and note that

$$K_j = K_1 J_j.$$

Calculation of $\{U_n\}$ and $\{V_n\}$

We can now modify the formulas for computing K_m and L_m above to get

$$\begin{aligned} J_{2j} &= 2J_jL_j, \\ L_{2j} &= L_j^2 + \tilde{\Delta}J_j^2 - 2, \\ J_{2j+1} &= L_{j+1}J_j + L_jJ_{j+1} - 1, \\ L_{2j+1} &= L_{j+1}L_j + \tilde{\Delta}J_{j+1}J_j - L_1, \end{aligned}$$

where $\tilde{\Delta} = \Delta K_1^2$.

Calculation of $\{U_n\}$ and $\{V_n\}$

We can now repeat the above strategy with $t = n$ and

$$\mathcal{W}_0 \equiv \{L_1, 1, L_2, J_2\} \pmod{M}.$$

Of course, we must replace Δ by $\tilde{\Delta}$ to compute

$$\mathcal{W}_h \equiv \{L_m, J_m, L_{m+1}, J_{m+1}\} \pmod{M}.$$

This technique requires about $1 + 9h$ modular multiplications modulo M to compute $J_m \equiv Q^{-n(m-1)} U_{2mn}/U_{2n}$ and $L_m \equiv V_{2mn}/Q^{mn} \pmod{M}$.

Primality test

As a consequence of results in §11.1 and §11.2 in William's "Edouard Lucas and Primality Testing", we know that if N is prime and q is a prime such that $q \equiv 1 \pmod 5$ and $N^{(q-1)/5} \not\equiv 1 \pmod q$, then if we put $\theta = (N^2+1)/5$,

$$P_1 = P(1,5,q), \quad P_2 = P(2,5,q), \quad Q = q^3,$$

where $P(i,r,q)$ is defined in (11.1.5), then

$$V_\theta / Q^{\theta/2} \equiv -1, \quad \Delta(U_\theta / Q^{\theta/2})^2 \equiv 5 \pmod N.$$

Primality test

we will use $\gamma_n(r)$ to denote that solution of $x^2 \equiv -1 \pmod{r^n}$ such that $0 < \gamma_n(r) < r^n$ and $\gamma_n(r)$ is odd.

The Test

Theorem

Let $N = A5^n + \eta\gamma_n(5)$, *where* $\eta^2 = 1$, $2 \mid A$ *and* $A < 2 \cdot 5^n$. *Suppose that* q *is a prime such that* $q \equiv 1 \pmod 5$ *and* $N^{(q-1)/5} \not\equiv 1 \pmod q$ *and let* P_1, P_2, Q *be defined as in previous slide. If we put*

$$R_0 \equiv S_0 \equiv U_{(N^2+1)/5^n}/2Q^{(N^2+1)/2\cdot 5^n},\ T_0 \equiv V_{(N^2+1)/5^n}/2Q^{(N^2+1)/2\cdot 5^n} \pmod N$$

and define

$$\begin{aligned} S_{i+1} &= S_i(\Delta^2 S_i^4 + 10\Delta S_i^2 T_i^2 + 5T_i^4 - 5\Delta S_i^2 - 15T_i^2 + 5) \pmod N, \\ T_{i+1} &= T_i(T_i^4 + 10\Delta S_i^2 T_i^2 + 5\Delta^2 S_i^4 - 5T_i^2 - 15\Delta S_i^2 + 5) \pmod N, \end{aligned}$$

for $i = 0, 1, 2, \ldots, n-1$, *then* N *is prime if and only if*

$$4\Delta S_{n-1}^2 \equiv 5 \pmod N \quad \textit{and} \quad 2T_{n-1} \equiv -1 \pmod N.$$

The End