Some New Pseudoprimes: A talk with too many slides and almost no punch line

Eric Roettger
Based on joint work with: Richard Guy and Hugh Williams

Mount Royal University

eroettger@mtroyal.ca

December 2013

Some Review

For our review I am roughly going to follow Hugh Williams' book "Édouard Lucas and Primality Testing", specifically Chapter 15. One of the first elementary number theory results you likely learned as an undergrad.

Theorem (Fermat's Little Theorem) If p is a prime, then

$$a^p \equiv a \pmod{p}.$$

Some Review

This is of course useful in the following way.
If N is a prime and $(a, N) = 1$, then

$$a^{N-1} \equiv 1 \pmod{N}.$$

Moreover, if we select a such that $(a, N) = 1$ and we find that

$$a^{N-1} \not\equiv 1 \pmod{N},$$

then we can say conclusively say N is not a prime.

Some Review

It is clear that, if we select a such that $(a, N) = 1$ and we find that

$$a^{N-1} \equiv 1 \pmod{N},$$

then we can not say conclusively say N is a prime. But it does give us some evidence that it might be the case.

Some Review

So we may be inclined to call this some sort of "Primality Test", but it certainly is not a "Primality Proof", as

$$2^{340} \equiv 1 \pmod{341},$$

and $341 = (11)(31)$.

Some Review

Definition We say that N is a base b pseudoprime (written b-psp or psp(b)) if N is composite integer such that

$$b^{N-1} \equiv 1 \pmod{N}.$$

Some Review

E. Malo. “Nombres qui, sans être premiers, vérifient exceptionellement une congruence de Fermat.” L’Intermédiaire des Math., 10:88, 1903. contains a proof of the infinitude of base 2 pseudoprimes.

Some Review

M. Cipolla. "Sui numeri composti P, che verificano la congruenza di Fermat $a^{P-1} \equiv 1 \pmod{P}$." ann. Mat. Pura Appl., 9:139-160, 1904. contains a proof of the infinitude of base b pseudoprimes for any base b.

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,

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

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

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

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

Fibonacci Pseudoprime

Emma Lehmer came up with the following definition.
Definition: A Fibonacci pseudoprime is a composite integer N such that

$$F_{N-\epsilon(N)} \equiv 0 \pmod{N},$$

where $\epsilon(N) = (\Delta/N)$.

The Infinitude of Fibonacci Pseudoprime

Emma Lehmer also showed that for an infinite number of primes p, $N = u_{2p}$ is a Fibonacci pseudoprime.

Lucas Pseudoprime

Definition: For a given pair of integers P, Q, we say that N is a Lucas pseudoprime if N is composite and

$$u_{N-\epsilon(N)}(P, Q) \equiv 0 \pmod{N},$$

where $\epsilon(N) = (\Delta/N)$ and $\Delta = P^2 - 4Q$.

Some Review

An example of a Fibonacci Pseudoprime (and thus also a Lucas Pseudoprime) is $N = 323 = (17)(19)$, here $(5/323) = -1$ and one can check that

$$F_{324} \equiv 0 \pmod{323} \quad \text{or} \quad u_{324}(1, -1) \equiv 0 \pmod{323}.$$

Infinitude of Lucas Pseudoprimes

In a 1973 paper A. Rotkiewicz showed that if $Q = \pm 1$ and P, Q are not both 1, there are infinitely many odd composite Lucas pseudoprimes with parameters P, Q.

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, $\ldots$ 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

$$X_{n+6m} = a_1 X_{n+5m} - a_2 X_{n+4m} + a_3 X_{n+3m} - a_4 X_{n+2m} + a_5 X_{n+m} - a_6 X_n,$$

where

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

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 $\omega | p - 1$.

Lucas Cubic Pseudoprime?

Definition: For a given set of integers P, Q, R we say that N is a Lucas cubic pseudoprime if N is composite and

$$C_{N-\epsilon(N)}(P,Q,R) \equiv 0 \pmod{N}, \quad \text{or}$$

$$C_{N^2+N+1}(P,Q,R) \equiv 0 \pmod{N},$$

where $\epsilon(N) = (\Delta/N)$ and $\Delta = Q^2P^2 - 4Q^3 - 4RP^3 + 18PQR - 27R^2$.

AN EXAMPLE S-prime like

An example of a Lucas Cubic Pseudoprime is $N = 533 = (13)(41)$, here $(\Delta/533) = 1$ and one can check that

$$C_{532}(1, -1, 1) \equiv 0 \pmod{533}.$$

AN EXAMPLE Q-prime like

An example of a Lucas Cubic Pseudoprime is $N = 407 = (11)(37)$, here $(\Delta/407) = -1$ and one can check that

$$C_{408}(1, -1, 13) \equiv 0 \pmod{407}.$$

A NONEXAMPLE

If $P = 1$, $Q = 2$ and $R = 3$, then there are no Lucas Cubic Pseudoprimes below 600.

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 $x^3 - S_1x^2 + S_2x + S_3$, 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

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

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

then

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

where α, β, γ are the zeros of $x^3 - P'x^2 + Q'x - R'$.

The Law of Apparition

Put $\Delta = S_1^2 - 4S_2 + 4RS_1 - 12R^2$. 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 $r \mid U_t$.

Another Lucas Cubic Pseudoprime

Defintion For a set of integers R, S_1, S_2, S_3, such that $S_3 = RS_1^2 - 2RS_2 - 4R^3$ we say N is a Lucas cubic pseudoprime if N is composite and

$$U_{N^2+\epsilon(N)N+1}(S_1, S_2, R) \equiv 0 \pmod{N} \quad \text{or}$$

$$U_{N-\epsilon(N)}(S_1, S_2, R) \equiv 0 \pmod{N},$$

where $\epsilon(N) = (\Delta/N)$ and $\Delta = S_1^2 - 4S_2 + 4RS_1 - 12R^2$.

AN EXAMPLE

An example of a Lucas Cubic Pseudoprime is $N = 329 = (7)(47)$, here $(\Delta/329) = -1$ and one can check that

$$U_{330}(1, 2, 3) \equiv 0 \pmod{329}.$$

AN EXAMPLE

An example of a Lucas Cubic Pseudoprime of the other kind is $N = 237 = (3)(79)$, here $(\Delta/237) = 1$ and one can check that

$$U_{56407}(-1, -7, 1) \equiv 0 \pmod{237}.$$

Note $237^2 + 237 + 1 = 56407$.

A NONEXAMPLE

If $S_1 = -1$, $S_2 = -5$ and $R = 1$ (Elkie's sequence), then there are no Lucas Cubic Pseudoprimes of this second type below 600.

AN EXAMPLE

An example of a Lucas Cubic Pseudoprime is $N = 1007 = (19)(53)$, here $(\Delta/1007) = -1$ and one can check that

$$U_{1008}(-1, -5, 1) \equiv 0 \pmod{1007}.$$

The End