Two Primality tests for Fermat numbers, based on Lucas Sequences.

Tony Reix (Tony.Reix@laposte.net)

2004, 10th of September

This paper provides the proof of two new primality tests for Fermat numbers, based on Lucas Sequences. The proofs are built by extending the properties and tests appearing in chapters 2.IV and 2.V of the famous book: "The Little Book of Bigger Primes" of Paulo Ribenboim. Though these chapters present the Lucas Sequences as a tool dedicated for proving the primality of $M-1$ numbers - like Mersenne numbers ($M_n = 2^q - 1$, where q is prime) - it seems that the properties appearing in these chapters can be *quite* easily extended to $M+1$ numbers, like Fermat numbers ($F_n = 2^{2^n} + 1$, where $n = 0, 1, 2, 3, ...$) . After providing the properties of the Lucas Sequence $U(4,3)$, I prove that: F_n prime $\Longrightarrow F_n \mid V_{\frac{N-1}{2}}$. Proving the converse then requires to provide a *generalized* version of several tests of chapter 2.V. I also show that it is a proof of Pepin's test, with $k = 3$. Finally, a computable version of the tests is given and their complexity is studied. Plus a guess.

1 Lucas Sequence $U(4,3)$

Let consider $(U_n)_{\ n\geqslant 0}$, a Lucas Sequence $U_n = PU_{n-1} - QU_{n-2}$ with $(P,Q) = (4,3)$ and with discriminant $D = P^2 - 4Q = 4 = 2^2$.

$$\text{We have: } \begin{cases} U_0 = 0 & U_1 = 1 & U_2 = \ 4 \\ V_0 = 2 & V_1 = P = 4 & V_2 = 10 \end{cases}$$

Table 5 page 62 provides more values of U_n and V_n .

The roots of the polynomial: $X^2 - PX + Q = X^2 - 4X + 3$ are α and β :

$$\left.\begin{matrix} \alpha \\ \beta \end{matrix}\right\} = \frac{P \pm \sqrt{D}}{2} = \begin{cases} 3 \\ 1 \end{cases}$$

$$\text{Thus, we have: } \begin{cases} U_n(4,3) & = & \dfrac{\alpha^n - \beta^n}{\alpha - \beta} & = & \dfrac{3^n - 1}{2} \\ V_n(4,3) & = & \alpha^n + \beta^n & = & 3^n + 1 \end{cases}$$

Then: $2U_n(U_n + 1) = 2 \times \frac{3^n - 1}{2} \times \big(\frac{3^n - 1}{2} + 1\big) = \frac{3^{2n} - 1}{2} = U_{2n}$.

And: $V_n(V_n - 2) + 2 = (3^n + 1)(3^n + 1 - 2) + 2 = 3^{2n} + 1 = V_{2n}$.

$$U_{2n} = 2U_n(U_n + 1) \tag{1}$$

$$V_{2n} = V_n(V_n - 2) + 2 \tag{2}$$

2 F_n prime $\implies F_n \mid V_{\frac{N-1}{2}}$

Let $F_n = 2^{2^n} + 1 = N$ be a prime, with $n \geq 1$ (and $N \geq 5$) .

By (IV.2) page 47 : $V_{2a} = V_a^2 - 2Q^{\,a}$ and with: $a = \frac{N-1}{2}$ we have:

$$V^2_{\frac{N-1}{2}} = V_{N-1} + \; 2Q^{\frac{N-1}{2}} \tag{3}$$

$$\text{Since:} \begin{cases} N \;\; \text{odd prime} \\ N = 2^{2^n} + 1 = (4)^{2^{n-1}} + 1 \equiv 2 \pmod 3 \\ ({}^{\mathrm{N}}\!/{}_{3}) = ({}^{2}\!/{}_{3}) = -1 \\ ({}^{3}\!/{}_{\mathrm{N}}) = ({}^{\mathrm{N}}\!/{}_{3}) \times (-1)^{\frac{3-1}{2}\frac{N-1}{2}} = (-1)(-1)^{2^{2^n-1}} = -1 \end{cases}$$

by the Euler quadratic residues congruence: $({}^{\mathrm{a}}\!/{}_{\mathrm{p}}) = a^{\frac{p-1}{2}} \pmod p$ page 34, and with $a = 3 = Q$ and $p = N$, we have: $Q^{\frac{N-1}{2}} \equiv -1 \pmod N$ and thus:

$$V^2_{\frac{N-1}{2}} \equiv V_{N-1} - 2 \pmod N. \tag{4}$$

$$\text{Since:} \begin{cases} ({}^{\mathrm{D}}\!/{}_{\mathrm{N}}) = ({}^{4}\!/{}_{\mathrm{N}}) = ({}^{2}\!/{}_{\mathrm{N}})^2 = 1 \\ N \text{ odd prime } > 3 \implies N \nmid 2QD \end{cases}$$

$$\text{by (IV.30) page 55 :} \begin{cases} U_{a+N-1} & \equiv & U_a & \pmod N \\ V_{a+N-1} & \equiv & V_a & \pmod N \end{cases} \quad \text{with } a = 0$$

$$\text{we have:} \begin{cases} U_{N-1} & \equiv & U_0 & \equiv & 0 & \pmod N \\ V_{N-1} & \equiv & V_0 & \equiv & 2 & \pmod N \end{cases}$$

And hence:

$$N \mid U_{N-1} \tag{5}$$

Since: $V^2_{\frac{N-1}{2}} \equiv 2 - 2 \equiv 0 \pmod N$, then we have:

$$N \mid V_{\frac{N-1}{2}} \tag{6}$$

3 Generalization of tests from Chapter 2.V

Now, for proving the converse, we will use a generalized version of the primality **Test 1** appearing page 66 of Ribenboim's book:

Generalized Test 1. Let $N > 1$ be an odd integer and $N - ({}^{\mathrm{D}}\!/_{\mathrm{N}}) = \prod_{i=1}^{s} q_i^{f_i}$. Assume that, for every prime factor q_i of $N - ({}^{\mathrm{D}}\!/_{\mathrm{N}})$, there exists a Lucas sequence $(U_n^{(i)})_{\ n \geq 0}$ with discriminant $D = P_i^2 - 4Q_i$, where $\gcd(P_i, Q_i) = 1$, or $\gcd(N, Q_i) = 1$, and such that $N \mid U^{(i)}_{N-({}^{\mathrm{D}}\!/_{\mathrm{N}})}$ and $N \nmid U^{(i)}_{\frac{N-({}^{\mathrm{D}}\!/_{\mathrm{N}})}{q_i}}$. Then N is prime.

The original test takes as a condition that $({}^{\mathrm{D}}\!/_{\mathrm{N}}) = -1$ and deals with the factorization of $N + 1$. We show that all properties and theorems used by Test 1 are valid when $({}^{\mathrm{D}}\!/_{\mathrm{N}}) = +1$ and that they apply to numbers N for which the factorization of $N - 1$ is known.

The proof of Test 1 makes use of the properties: (V.1), (V.2), (V.3), (V.4), and also of (IV.29) or (IV.22) which do not depend on the value of $({}^{\mathrm{D}}\!/_{\mathrm{N}})$.

(V.1). If N is odd, $\gcd(N, D) = 1$, then $\Psi_D(N) = N - ({}^{\mathrm{D}}\!/_{\mathrm{N}})$ if and only if N is a prime.

(V.1) does not depend on the value of $({}^{\mathrm{D}}\!/_{\mathrm{N}})$. The proof of (V.1) requires N is odd but it does not depend on the value of $({}^{\mathrm{D}}\!/_{\mathrm{N}})$: $\Psi_D(N) < N-1 < N+1$ and thus: $\Psi_D(N) < N - ({}^{\mathrm{D}}\!/_{\mathrm{N}})$.

(V.2). If N is odd, $\gcd(N, D) = 1$, and $N - ({}^{\mathrm{D}}\!/_{\mathrm{N}})$ divides $\Psi_D(N)$, then N is prime.

The proof uses the hypothesis: $({}^{\mathrm{D}}\!/_{\mathrm{N}}) \leq 1$ which is true for $({}^{\mathrm{D}}\!/_{\mathrm{N}}) = \mp 1$, and it uses (V.1) which does not depend on the value of $({}^{\mathrm{D}}\!/_{\mathrm{N}})$.

(V.3). If N is odd, $U = U(P, Q)$ is a Lucas sequence with discriminant D, and $\gcd(N, QD) = 1$, then N divides $U_{\Psi_D(N)}$.

The proof of (V.3) makes use of (IV.19), (IV.20) and (IV.21), which do not depend on the value of $({}^{\mathrm{D}}\!/_{\mathrm{N}})$.

Generalized (V.4). If N is odd and $U = U(P, Q)$ is a Lucas sequence with discriminant D such that N divides $U_{N-({}^{\mathrm{D}}\!/_{\mathrm{N}})}$, then $\gcd(N, QD) = 1$.

The proof of (V.4) makes use of the property: $({}^{\mathrm{D}}\!/_{\mathrm{N}}) \neq 0$, and of (IV.19) which does not depend on the value of $({}^{\mathrm{D}}\!/_{\mathrm{N}})$. Thus (V.4) can be generalized.

4 $F_n \mid V_{\frac{N-1}{2}} \implies F_n$ is prime

Let $F_n = 2^{2^n} + 1 = N$, with $n \geq 1$ (and $N \geq 5$) .

Assume that N divides $V_{\frac{N-1}{2}}$.
By (IV.2) page 47: $U_{2n} = U_n V_n$, we have: $N \mid U_{N-1}$.
With the Lucas sequence $U = U(4,3)$, with discriminant $D = 4$, we have:

$$U_{a+1} = 4U_a - 3U_{a-1} \tag{7}$$

We have: $$3U_a + 1 = \frac{3^{a+1} - 3 + 2}{2} = \frac{3^{a+1} - 1}{2} = U_{a+1} \tag{8}$$

and : $$3V_a - 2 = 3^{a+1} + 3 - 2 = 3^{a+1} + 1 = V_{a+1} \tag{9}$$

By (1) U_{2a} is even. Since U_0 is even, by (8) U_{2a+1} is odd.

By (IV.5.b) page 47: $V_b = 2U_{b+1} - PU_b = 2(U_{b+1} - 2U_b)$, and thus:

$$V_b = 2(3U_b + 1 - 2U_b) = 2(U_b + 1)$$

$$\text{and: } \begin{cases} \gcd(V_b, U_b) = 2 \text{ when } b \text{ is even.} \\ \gcd(V_b, U_b) = 1 \text{ when } b \text{ is odd.} \end{cases}$$

Since $({}^{\mathrm{D}}\!/_{\mathrm{N}}) = 1$, we have: $\gcd(N, D) = 1$.

With $n \geq 1$, we have shown in **2** that $N = 2^{2^n} + 1 \equiv 2 \pmod 3$.

Since N is odd, since $N \mid V_{\frac{N-1}{2}}$, and since $\gcd(V_a, U_a)$ is 1 or 2,

$$\text{then we have: } \begin{cases} \gcd(N, U_{\frac{N-1}{2}}) & = 1 \quad \text{and thus:} \quad N \nmid U_{\frac{N-1}{2}} \\ \gcd(N, 2) & = 1 \end{cases}$$

$N > 1$ is odd and $N - 1 = 2^q$.
For 2 - the unic prime factor of $N - ({}^{\mathrm{D}}\!/_{\mathrm{N}})$ - there exists a Lucas sequence U with $(P,Q) = (4,3)$ and with discriminant $D = P^2 - 4Q = 4$ such that $({}^{\mathrm{D}}\!/_{\mathrm{N}}) = 1$, with $\gcd(P,Q) = 1$ and $\gcd(N,2) = 1$.
By **Generalized Test 1**, since $N \mid U_{N-1}$ but $N \nmid U_{\frac{N-1}{2}}$, N is a prime.

And Finally we have the following theorem:

Theorem 1 $F_n = 2^{2^n} + 1$ *(*$n \geqslant 1$*) is a prime if and only if it divides* $V_{\frac{F_n-1}{2}}$.

Since $V_n = 3^n + 1$ as shown in page 1, and by the previous theorem, we have: $F_n = 2^{2^n} + 1$ ($n \geqslant 1$) is a prime if and only $3^{\frac{N-1}{2}} \equiv -1 \pmod{F_n}$, which is the Pepin's test for $k = 3$, page 71.

5 Two primality tests for Fermat numbers

It is convenient to replace the Lucas sequences $(V_n)_{\ n\geq 0}$ and $(U_n)_{\ n\geq 0}$ by the following sequences $(S_k)_{\ k\geq 0}$ and $(T_k)_{\ k\geq 0}$ defined recursively as follows:

$$\begin{cases} S_0 = V_1 = 4, \quad & S_{k+1} = S_k(S_k - 2) + 2 \\ T_0 = U_1 = 1, \quad & T_{k+1} = 2T_k(T_k + 1) \end{cases}$$

Assume that $S_{k-1} = V_{2^{k-1}}$; then, for $k > 1$, by (2) we have:

$$S_k = S_{k-1}(S_{k-1} - 2) + 2 = V_{2^{k-1}}(V_{2^{k-1}} - 2) + 2 = V_{2\times 2^{k-1}} = V_{2^k}$$

By theorem 1, F_n is prime if and only if F_n divides: $V_{\frac{F_n - 1}{2}} = V_{2^{2^n - 1}} = S_{2^n - 1}$, or equivalently if: $S_{2^n-1} \equiv 0 \pmod{F_n}$.

Thus we have the following theorem:

Theorem 2 (Lucas-Lehmer-Ribenboim-Reix-1)
$F_n = 2^{2^n} + 1$ ($n \geqslant 1$) is a prime if and only if it divides S_{2^n-1} , where $S_0 = 4$ and $S_k = S_{k-1}(S_{k-1} - 2) + 2$, for $k = 1, 2, 3, ..., 2^n - 1$.

Assume that $T_{k-1} = U_{2^{k-1}}$; then, for $k > 1$, by (1) we have:

$$T_k = 2T_{k-1}(T_{k-1} + 1) = 2U_{2^{k-1}}(U_{2^{k-1}} + 1) = U_{2\times 2^{k-1}} = U_{2^k}$$

By theorem 1, F_n is prime if and only if F_n divides: $V_{\frac{F_n - 1}{2}} = V_{2^{2^n - 1}} = 2(U_{2^{2^n-1}} + 1) = 2(T_{2^n-1} + 1)$, or equivalently if: $T_{2^n-1} \equiv -1 \pmod{F_n}$.

Since $T_x = -1$ entails $2T_x(T_x + 1) = 0$, thus we have the following theorem:

Theorem 3 (Lucas-Lehmer-Ribenboim-Reix-2)
$F_n = 2^{2^n} + 1$ ($n \geqslant 1$) is a prime if and only if it divides T_{2^n} , where $T_0 = 1$ and $T_k = 2T_{k-1}(T_{k-1} + 1)$, for $k = 1, 2, 3, ..., 2^n$.

6 Numerical Examples

$$\begin{aligned}
&\pmod{F_2}\ S_0 = 4 \overset{1}{\mapsto} \mathbf{10} \overset{2}{\mapsto} \mathbf{14} \overset{3}{\mapsto} S_{2^2-1} \equiv 0 \\
&\pmod{F_3}\ S_0 = 4 \overset{1}{\mapsto} 10 \overset{2}{\mapsto} 82 \overset{3}{\mapsto} 137 \overset{4}{\mapsto} \mathbf{250} \overset{5}{\mapsto} \mathbf{65} \overset{6}{\mapsto} 242 \overset{7}{\mapsto} S_{2^3-1} \equiv 0 \\
&\pmod{F_4}\ S_0 = 4 \overset{1}{\mapsto} 10 \cdots \overset{11}{\mapsto} \mathbf{65530} \overset{12}{\mapsto} \mathbf{65} \overset{13}{\mapsto} 4097 \overset{14}{\mapsto} 65282 \overset{15}{\mapsto} S_{2^4-1} \equiv 0
\end{aligned}$$

$$\begin{aligned}
&\pmod{F_2}\ T_0 = 1 \overset{1}{\mapsto} \mathbf{4} \overset{2}{\mapsto} 6 \overset{3}{\mapsto} 16 \overset{4}{\mapsto} T_{2^2} \equiv 0 \\
&\pmod{F_3}\ T_0 = 1 \overset{1}{\mapsto} 4 \overset{2}{\mapsto} 40 \overset{3}{\mapsto} 196 \overset{4}{\mapsto} \mathbf{124} \overset{5}{\mapsto} 160 \overset{6}{\mapsto} 120 \overset{7}{\mapsto} 256 \overset{8}{\mapsto} T_{2^3} \equiv 0 \\
&\pmod{F_4}\ T_0 = 1 \overset{1}{\mapsto} 4 \overset{2}{\mapsto} 40\ \cdots \overset{11}{\mapsto} \mathbf{32764}\ \cdots \overset{14}{\mapsto} 32640 \overset{15}{\mapsto} 65536 \overset{16}{\mapsto} T_{2^4} \equiv 0
\end{aligned}$$

7 Complexity

The primality tests **LLRR-1** and **LLRR-2** are based on the computation of the 2 functions: $f_1 : x \longmapsto x^2 - 2x + 2$ and $f_2 : x \longmapsto 2x^2 + 2x$.

Though these functions seem to require more computation than the **LLT**: $x \longmapsto x^2 - 2$, the cost of their computation is comparable to the cost of computing **LLT** : in addition to squaring x and adding/substracting 2, they only require to multiply x or/and x^2 by 2 which is done easily and quickly by binary left shifting.

8 Conjectured properties

For $n = 2, 3, 4$ we have: $S_{2^n-n-1} \equiv F_n - 7 \pmod{F_n}$, $S_{2^n-n} \equiv 65 \pmod{F_n}$.
For $n = 5...13$ we have: $S_{2^n-n-1} \not\equiv F_n - 7 \pmod{F_n}$, $S_{2^n-n} \not\equiv 65 \pmod{F_n}$.
For $n = 2, 3...13$ with $S_0 = 65$, we have: $S_{n-1} \equiv 0 \pmod{F_n}$.

Thus we have the following conjecture:

Conjecture 1
$F_n = 2^{2^n} + 1$ $(n \geqslant 2)$ is a prime if and only if it divides $S_{2^n-n-1} + 7$, where $S_0 = 4$ and $S_k = S_{k-1}(S_{k-1} - 2) + 2$, for $k = 1, 2, 3, ..., 2^n - n - 1$.

For $n = 2, 3, 4$ we have: $T_{2^n-n-1} \equiv 2^{2^n-1} - 4 \pmod{F_n}$.
For $n = 5...13$ we have: $T_{2^n-n-1} \not\equiv 2^{2^n-1} - 4 \pmod{F_n}$.
For $n = 2, 3...13$ with $T_0 = 2^{2^n-1} - 4$, we have: $T_{n+1} \equiv 0 \pmod{F_n}$.

Thus we have the following conjecture:

Conjecture 2
$F_n = 2^{2^n} + 1$ $(n \geqslant 2)$ is a prime if and only if it divides $T_{2^n-n-1} - 2^{2^n-1} + 4$, where $T_0 = 1$ and $T_k = 2T_{k-1}(T_{k-1} + 2)$, for $k = 1, 2, 3, ..., 2^n - n - 1$.

Since 2^n grows much faster than n, these conjectures can not reduce the time needed for proving that a big Fermat number, like F_{33}, is prime or not.

9 Conclusion

The *fixed points* $S_{2^n-n} = 65$ and $T_{2^n-n-1} = 2^{2^n-1} - 4$ are very noticeable.

It is my opinion that it may exist other Lucas-Lehmer-like tests providing more interesting fixed points - something like: $S_{2^{n-1}} = C$ - that would reduce the time needed by Pepin's test for proving that a Fermat number is a prime or not.