A LLT-like test for proving the primality of Fermat numbers.

Tony Reix (Tony.Reix@laposte.net)
First version: 2004, 24th of September ; Updated: 2005, 19th of October

This paper provides a proof of:

Theorem 1 (Lucas-Lehmer-Williams-Reix-1)
$F_n = 2^{2^n} + 1$ $(n \geqslant 1)$ is a prime if and only if it divides S_{2^n-2} , where $S_0 = 5$ and $S_i = S_{i-1}^2 - 2$ for $i = 1, 2, 3, ...\ 2^n - 1$.

The proof is based on the chapters 4 (The Lucas Functions) and 8.4 (The Lehmer Functions) of the book "Édouard Lucas and Primality Testing" of H. C. Williams, 1998.
Chapter 1 explains how the (P, Q) parameters have been found. Then Chapter 2 provides the Lehmer theorems used for the proof. Then, Chapter 3 and 4 provide the proof for: F_n prime $\Longrightarrow F_n \mid S_{2^n-2}$ and the converse, proving theorem 1. Chapter 5 provides numerical examples. The appendix in Chapter 6 provides first values of U_n and V_n plus some properties.

1 Lucas Sequence with $P = \sqrt{R}$

Let $S_0 = 5$ and $S_i = S_{i-1}^2 - 2$. $S_1 = 23$, $S_2 = 527 = 17 \times 31$, ...

It has been checked that: $\begin{cases} S_{2^n-2} \equiv 0 \pmod{F_n} & \text{for } n = 1...4 \\ S_{2^n-2} \not\equiv 0 \pmod{F_n} & \text{for } n = 5...14 \end{cases}$

Here after, we search a Lucas Sequence $(U_m)_{m \geqslant 0}$ and its companion $(V_m)_{m \geqslant 0}$ with (P, Q) that fit with the values of the S_i sequence.

We define the Lucas Sequence V_m such that:

$$V_{2^{k+1}} = S_k \tag{1}$$

Thus we have: $\begin{cases} V_2 & = & S_0 & = & 5 \\ V_4 & = & S_1 & = & 23 \\ V_8 & = & S_2 & = & 527 \end{cases}$

If (4.2.7) page 74 ($V_{2n} = V_n^2 - 2Q^n$) applies, we have: $\begin{cases} V_4 = V_2^2 - 2Q^2 \\ V_8 = V_4^2 - 2Q^4 \end{cases}$

and thus: $Q = \sqrt[2]{\frac{V_2^2 - V_4}{2}} = \sqrt[4]{\frac{V_4^2 - V_8}{2}} = \pm 1$.

With (4.1.3) page 70 ($V_{n+1} = PV_n - QV_{n-1}$), and with:

$$\begin{cases} V_0 = 2 \\ V_1 = P \\ V_2 = PV_1 - QV_0 = P^2 - 2Q \end{cases}$$

we have: $P = \sqrt{V_2 + 2Q} = \sqrt{7}$ or $\sqrt{3}$.
In the following we consider: $(P, Q) = (\sqrt{7}, 1)$.

As explained by Williams page 196, "all of the identity relations [Lucas functions] given in (4.2) continue to hold, as these are true quite without regard as to whether P, Q are integers".

So, like Lehmer, we define $P = \sqrt{R}$ such that $R = 7$ and $Q = 1$ are coprime integers and we define (Property (8.4.1) page 196):

$$\overline{V}_n = \begin{cases} V_n & \text{when } 2 \mid n \\ V_n/\sqrt{R} & \text{when } 2 \nmid n \end{cases} \qquad \overline{U}_n = \begin{cases} U_n/\sqrt{R} & \text{when } 2 \mid n \\ U_n & \text{when } 2 \nmid n \end{cases}$$

in such a way that $\overline{V}_n$ and $\overline{U}_n$ are always integers.

Tables 1 to 5 give values of U_i , V_i , $\overline{U}_i \pmod{F_n}$, $\overline{V}_i \pmod{F_n}$, with $(P, Q) = (\sqrt{7}, 1)$, for $n = 1, 2, 3, 4$.

2 Lehmer theorems

Like Lehmer, let define the symbols (where $\left(a/b\right)$ is the Legendre symbol) :

$$\begin{cases} \varepsilon = \varepsilon(p) = \left(D/p\right) \\ \sigma = \sigma(p) = \left(R/p\right) \\ \tau = \tau(p) = \left(Q/p\right) \end{cases}$$

The 2 following formulas (from page 77) will help proving properties:

$$(4.2.28) \qquad 2^{m-1} U_{mn} = \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \binom{m}{2i+1} D^i U_n^{2i+1} V_n^{m-(2i+1)}$$

$$(4.2.29) \qquad 2^{m-1} V_{mn} = \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \binom{m}{2i} D^i U_n^{2i} V_n^{m-2i}$$

Property (8.4.2) page 196 :

If p is an odd prime and $p \nmid Q$, then: $\begin{cases} \overline{U}_p \equiv \left(D/p\right) \pmod{p} \\ \overline{V}_p \equiv \left(R/p\right) \pmod{p} \end{cases}$

Proof:
Since p is a prime, and by Fermat little theorem, we have: $2^{p-1} \equiv 1 \pmod{p}$.

- By (4.2.28), with $m = p$ and $n = 1$, since $U_1 = 1$ and $V_1 = P$, we have:

$$2^{p-1} U_p = \sum_{i=0}^{\frac{p-1}{2}} \binom{p}{2i+1} D^i U_1^{2i+1} V_1^{p-(2i+1)}$$

$$2^{p-1}U_p = \binom{p}{1}P^{p-1} + \binom{p}{3}DP^{p-3} + ... + \binom{p}{p}D^{\frac{p-1}{2}}P^0$$

Since $\binom{p}{i} \equiv 0 \pmod{p}$ when $0 < i < p$ and $\binom{p}{p} = 1$, we have:

$$U_p = \overline{U}_p \equiv D^{\frac{p-1}{2}} \equiv \left(\mathrm{D}/\mathrm{p}\right) \pmod{p}$$

- By (4.2.29), with $m = p$ and $n = 1$, since $U_1 = 1$ and $V_1 = P$, we have:

$$2^{p-1}V_p = \sum_{i=0}^{\frac{p-1}{2}} \binom{p}{2i} D^i U_1^{2i} V_1^{p-2i}$$

$$2^{p-1}V_p = \binom{p}{0}P^p + \binom{p}{2}DP^{p-2} + ... + \binom{p}{p-1}D^{\frac{p-1}{2}}P$$

Since $\binom{p}{0} = 1$, and $\binom{p}{i} \equiv 0 \pmod{p}$ when $0 < i < p$, we have:

$$V_p \equiv P^p \text{ and } \overline{V}_p \equiv P^{p-1} \equiv R^{\frac{p-1}{2}} \equiv \left(\mathrm{R}/\mathrm{p}\right) \pmod{p}$$

□

Property (8.4.3) page 197 :

$$p \text{ odd prime and } p \nmid Q \Longrightarrow p \mid \overline{U}_{p-\sigma\varepsilon}$$

Proof

By (4.2.28) with $n = 1$, $V_1 = P$, since p is a prime and $(R, Q) = 1$, we have:

- With: $m = p + 1$

$$2^p U_{p+1} = \sum_{i=0}^{\frac{p+1}{2}} \binom{p+1}{2i+1} D^i P^{p-2i}$$

$$2^p U_{p+1} = \binom{p+1}{1}P^p + \binom{p+1}{3}DP^{p-2} + ... + \binom{p+1}{p}D^{\frac{p-1}{2}}P + \binom{p+1}{p+2}D^{\frac{p+1}{2}}P^{-1}$$

$$2^p U_{p+1} = (p+1)P^p + (p+1)p[...] + (p+1)D^{\frac{p-1}{2}}P + 0D^{\frac{p+1}{2}}P^{-1}$$

$$2^p U_{p+1} = P^p + D^{\frac{p-1}{2}}P + p[...] = P\left[(P^2)^{\frac{p-1}{2}} + D^{\frac{p-1}{2}}\right] + p[...]$$

$$\frac{2^p U_{p+1}}{P} = 2^p \overline{U}_{p+1} \equiv R^{\frac{p-1}{2}} + D^{\frac{p-1}{2}} \equiv \left(\mathrm{R}/\mathrm{p}\right) + \left(\mathrm{D}/\mathrm{p}\right) = \sigma(p) + \varepsilon(p) \pmod{p}$$

Thus, if $\sigma\varepsilon = \sigma(p) \times \varepsilon(p) = -1$, then $p \mid \overline{U}_{p+1} = \overline{U}_{p-\sigma\epsilon}$.

- With: $m = p-1$:

$$2^{p-2}U_{p-1} = \sum_{i=0}^{\frac{p-1}{2}} \binom{p-1}{2i+1} D^i P^{p-2(i+1)}$$

$$2^{p-2}U_{p-1} = \binom{p-1}{1} P^{p-2} + \binom{p-1}{3} DP^{p-4} + ... + \binom{p-1}{p-2} D^{\frac{p-3}{2}} P + \binom{p-1}{p} D^{\frac{p-1}{2}} P^{-1}$$

$$2^{p-2}U_{p-1} = (p-1)P^{p-2} + (p-1)DP^{p-4} + ... + (p-1)D^{\frac{p-3}{2}} P + 0D^{\frac{p-1}{2}} P^{-1}$$

$$\frac{2^{p-2}U_{p-1}}{P} \equiv -[P^{p-3} + DP^{p-5} + ... \ + D^{\frac{p-3}{2}}] \equiv -\frac{P^{p-1} - D^{\frac{p-1}{2}}}{P^2 - D} \pmod p$$

$$2^{p-2}\overline{U}_{p-1}(P^2 - D) \equiv -(P^2)^{\frac{p-1}{2}} + D^{\frac{p-1}{2}} \equiv \varepsilon(p) - \sigma(p) \pmod p$$

Thus, if $\sigma\varepsilon = \sigma(p) \times \varepsilon(p) = 1$, then $p \mid \overline{U}_{p-1} = \overline{U}_{p-\sigma\epsilon}$.

□

Property (8.4.4) page 197

If p is an odd prime and $p \nmid Q$, then: $V_{p-\sigma\varepsilon} \equiv 2\sigma Q^{\frac{1-\sigma\varepsilon}{2}} \pmod p$

Theorem 2 (8.4.1) *If p is an odd prime and $p \nmid QRD$, then:*

$$\begin{cases} p \mid \overline{V}_{\frac{p-\sigma\epsilon}{2}} & \textit{when} \quad \sigma = -\tau \\ p \mid \overline{U}_{\frac{p-\sigma\epsilon}{2}} & \textit{when} \quad \sigma = \tau \end{cases}$$

Definition (8.4.2) page 197 of $\omega(m)$: For a given m, denote by $\omega = \omega(m)$ the value of the least positive integer k such that $m \mid \overline{U}_k$. If $\omega(m)$ exists, $\omega(m)$ is called the **rank of apparition** of m .

Theorem 3 (8.4.3)

$$\begin{cases} \textit{If } k \mid n, \textit{ then } \overline{U}_k \mid \overline{U}_n \ . \\ \textit{If } m \mid \overline{U}_n, \textit{ then } \omega(m) \mid n \ . \end{cases}$$

Theorem 4 (8.4.5) *If $(m, Q) = 1$, then $\omega(m)$ exists.*

Theorem 5 (8.4.6) *If $(N, 2QRD) = 1$ and $N \pm 1$ is the rank of apparition of N, then N is a prime.*

Theorem 6 (8.4.7) *If* $(N, 2QRD) = 1$, $\overline{U}_{N\pm 1} \equiv 0 \pmod N$ *and* $\overline{U}_{\frac{N\pm1}{q}} \not\equiv 0 \pmod N$ *for each distinct prime divisor* q *of* $N \pm 1$*, then* N *is a prime.*

Proof:
Let $\omega = \omega(N)$. We see that $\omega \mid N \pm 1$, but $\omega \nmid (N \pm 1)/q$. Thus if $q^\alpha \parallel N \pm 1$, then $q^\alpha \mid \omega$. It follows that $\omega = N \pm 1$ and N is a prime by Theorem 5 (8.4.6) .

3 F_n prime $\Longrightarrow F_n \mid \overline{V}_{\frac{F_n-1}{2}}$ and $F_n \mid S_{2^n-2}$

Let $N = F_n = 2^{2^n} + 1$ with $n \geq 1$ be an odd prime.
Let: $P = \sqrt{R}$, $R = 7$, $Q = 1$, and $D = P^2 - 4Q = 3$.

Hereafter we compute $\left({}^3\!/\!_N\right)$ and $\left({}^7\!/\!_N\right)$:

- $\left({}^3\!/\!_N\right)$:

$$\text{Since: } \begin{cases} N \ \text{ odd prime} \\ N = (4)^{2^{n-1}} + 1 \equiv 2 \pmod 3 \\ \left({}^N\!/\!_3\right) = \left({}^2\!/\!_3\right) = -1 \\ \left({}^3\!/\!_N\right) = \left({}^N\!/\!_3\right) \times (-1)^{\frac{3-1}{2}\frac{N-1}{2}} \end{cases} \qquad \text{then: } \left({}^3\!/\!_N\right) = -1 \ .$$

- $\left({}^7\!/\!_N\right)$: We have:

$$\begin{cases} 2^3 & \equiv & 1 & \pmod 7 \\ 2^{3a+b} & \equiv & 2^b & \pmod 7 \end{cases}$$

With $2^n \equiv b \pmod 3$, we have: $2^{2^n} + 1 \equiv 2^b + 1 \pmod 7$. Then we study the exponents of 2, modulo 3 . We have: $2^2 \equiv 1 \pmod 3$, and:

$$\text{If } n = 2m \qquad \begin{cases} 2^{2m} \equiv 1 \pmod 3 \\ N = 2^{2^{2m}} + 1 \equiv 2^1 + 1 \equiv 3 \pmod 7 \\ \left({}^N\!/\!_7\right) = \left({}^3\!/\!_7\right) = -1 \end{cases}$$

$$\text{If } n = 2m+1 \ \begin{cases} 2^{2m+1} \equiv 2 \pmod 3 \\ N = 2^{2^{2m+1}} + 1 \equiv 2^2 + 1 \equiv 5 \pmod 7 \\ \left({}^N\!/\!_7\right) = \left({}^5\!/\!_7\right) = -1 \end{cases}$$

Finally, we have: $\left({}^7\!/\!_N\right) = \left({}^N\!/\!_7\right)(-1)^{\frac{7-1}{2}2^{2^n}} = \left({}^N\!/\!_7\right) = -1$.

$$\text{So we have: } \begin{cases} \varepsilon = \left({}^D\!/\!_N\right) = \left({}^3\!/\!_N\right) = & -1 \\ \sigma = \left({}^R\!/\!_N\right) = \left({}^7\!/\!_N\right) = & -1 \\ \tau = \left({}^Q\!/\!_N\right) = \left({}^1\!/\!_N\right) = & +1 \end{cases}$$

Since $\sigma = -\tau$, $\sigma\epsilon = +1$, and $F_n \nmid QRD$ with $n \geq 1$, then by Theorem 2 (8.4.1) we have:

$$F_n \text{ prime } \Longrightarrow F_n \mid \overline{V}_{\frac{F_n-1}{2}} = V_{2^{2^n-1}}$$

By (1) we have: $V_{2^{k-1}} = S_{k-2}$ and thus, with $k = 2^n$: $F_n \mid S_{2^n-2}$.

□

4 $F_n \mid S_{2^n-2} \Longrightarrow F_n$ is a prime

Let $N = F_n$ with $n \geq 1$. By (1) we have: $N \mid S_{2^n-2} \Longrightarrow N \mid V_{2^{2^n-1}}$.

And thus, by (4.2.6) page 74 ($U_{2a} = U_a V_a$) , we have: $N \mid \overline{U}_{2^{2^n}}$.

By (4.3.6) page 85: ($(V_n, U_n) \mid 2Q^n$ for any n), and since $Q = 1$, then: $(V_{2^{2^n-1}}, \overline{U}_{2^{2^n-1}}) = 2$ and thus: $N \nmid \overline{U}_{2^{2^n-1}}$ since N odd.

With $\omega = \omega(N)$, by Theorem 3 (8.4.3) we have : $\omega \mid 2^{2^n}$ and $\omega \nmid 2^{2^n-1}$.

This implies: $\omega = 2^{2^n} = N - 1$. Then $N - 1$ is the rank of apparition of N, and thus by Theorem 5 (8.4.6) N is a prime.

□

5 Numerical Examples

(mod F_2) $S_0 = 5 \overset{1}{\mapsto} 6 \overset{2}{\mapsto} S_{2^2-2} \equiv 0$
(mod F_3) $S_0 = 5 \overset{1}{\mapsto} 23 \overset{2}{\mapsto} 13 \overset{3}{\mapsto} 167 \overset{4}{\mapsto} 131 \overset{5}{\mapsto} 197 = -60 \overset{6}{\mapsto} S_{2^3-2} \equiv 0$
(mod F_4) $S_0 = 5 \overset{1}{\mapsto} 23 \overset{2}{\mapsto} 527 \overset{3}{\mapsto} 15579 \overset{4}{\mapsto} 21728 \overset{5}{\mapsto} 42971 \overset{6}{\mapsto} 1864 \overset{7}{\mapsto} 1033 \overset{8}{\mapsto} 18495 \overset{9}{\mapsto} 27420 \overset{10}{\mapsto} 15934 \overset{11}{\mapsto} 2016 \overset{12}{\mapsto} 960 \overset{13}{\mapsto} 4080 \overset{14}{\mapsto} S_{2^4-2} \equiv 0$

6 Appendix: Table of U_i and V_i

With $n = 2, 3, 4$, we have the following (not proven) properties (modulo F_n):

$$\begin{cases} \overline{U}_{F_n-5} & \equiv & 5 \\ \overline{U}_{F_n-4} & \equiv & 6 \\ \overline{U}_{F_n-3} & \equiv & 1 \\ \overline{U}_{F_n-2} & \equiv & 1 \\ \overline{U}_{F_n-1} & \equiv & 0 \\ \overline{U}_{F_n} & \equiv & -1 \\ \overline{U}_{F_n+1} & \equiv & -1 \\ \overline{U}_{F_n+2} & \equiv & -6 \\ \overline{U}_{F_n+3} & \equiv & -5 \end{cases} \qquad \begin{cases} \overline{V}_{F_n-5} & \equiv & -23 \\ \overline{V}_{F_n-4} & \equiv & -4 \\ \overline{V}_{F_n-3} & \equiv & -5 \\ \overline{V}_{F_n-2} & \equiv & -1 \\ \overline{V}_{F_n-1} & \equiv & -2 \\ \overline{V}_{F_n} & \equiv & -1 \\ \overline{V}_{F_n+1} & \equiv & -5 \\ \overline{V}_{F_n+2} & \equiv & -4 \\ \overline{V}_{F_n+3} & \equiv & -23 \end{cases}$$

i	U_i		V_i	
0	0	$\times\sqrt{7}$	2	
1	1		1	$\times\sqrt{7}$
2	1	$\times\sqrt{7}$	5	
3	6		4	$\times\sqrt{7}$
4	5	$\times\sqrt{7}$	23	
5	29		19	$\times\sqrt{7}$
6	24	$\times\sqrt{7}$	110	
7	139		91	$\times\sqrt{7}$
8	115	$\times\sqrt{7}$	527	
9	666		436	$\times\sqrt{7}$
10	551	$\times\sqrt{7}$	2525	
11	3191		2089	$\times\sqrt{7}$
12	2640	$\times\sqrt{7}$	12098	
13	15289		10009	$\times\sqrt{7}$
14	12649	$\times\sqrt{7}$	57965	
15	73254		47956	$\times\sqrt{7}$
16	60605	$\times\sqrt{7}$	277727	
17	350981		229771	$\times\sqrt{7}$
18	290376	$\times\sqrt{7}$	1330670	
19	1681651		1100899	$\times\sqrt{7}$
20	1391275	$\times\sqrt{7}$	6375623	
21	8057274		5274724	$\times\sqrt{7}$
22	6665999	$\times\sqrt{7}$	30547445	
23	38604719		25272721	$\times\sqrt{7}$
24	31938720	$\times\sqrt{7}$	146361602	
25	184966321		121088881	$\times\sqrt{7}$
26	153027601	$\times\sqrt{7}$	701260565	
27	886226886		580171684	$\times\sqrt{7}$
28	733199285	$\times\sqrt{7}$	3359941223	
29	4246168109		2779769539	$\times\sqrt{7}$
30	3512968824	$\times\sqrt{7}$	16098445550	
31	20344613659		13318676011	$\times\sqrt{7}$
32	16831644835	$\times\sqrt{7}$	77132286527	
33	97476900186		63813610516	$\times\sqrt{7}$
34	80645255351	$\times\sqrt{7}$	369562987085	
35	467039887271		305749376569	$\times\sqrt{7}$
36	386394631920	$\times\sqrt{7}$	1770682648898	
37	2237722536169		1464933272329	$\times\sqrt{7}$
38	1851327904249	$\times\sqrt{7}$	8483850257405	
39	10721572793574		7018916985076	$\times\sqrt{7}$
40	8870244889325	$\times\sqrt{7}$	40648568638127	

Table 1: $P =_7\sqrt{7}$, $Q = 1$

i	$\overline{U}_i \pmod{F_1}$	$\overline{V}_i \pmod{F_1}$
0	0	2
1	1	1
2	1	**0**
3	1	4
4	**0**	3
5	4	4
6	4	0
7	4	1
8	0	2

Table 2: $P = \sqrt{7}$, $Q = 1$, Modulo F_1

i	$\overline{U}_i \pmod{F_2}$	$\overline{V}_i \pmod{F_2}$
0	0	2
1	1	1
2	1	5
3	6	4
4	5	6
5	12	2
6	7	8
7	3	6
8	13	**0**
9	3	11
10	7	9
11	12	15
12	5	11
13	6	-4
14	1	-5
15	1	-1
16	**0**	-2
17	-1	-1
18	-1	-5
19	-6	-4
20	-5	11
21	5	15
22	10	9
23	14	11
24	4	0

Table 3: $P = \sqrt{7}$, $Q = 1$, Modulo F_2

i	$\overline{U}_i \pmod{F_3}$	$\overline{V}_i \pmod{F_3}$
0	0	2
1	1	1
2	1	5
3	6	4
4	5	23
8	115	13
16	210	167
32	118	131
64	38	197
128	33	**0**
192	38	60
224	118	126
240	210	90
248	115	-13
252	5	-23
253	6	-4
254	1	-5
255	1	-1
256	**0**	-2
257	-1	-1
258	-1	-5
259	-6	-4
260	-5	-23

Table 4: $P = \sqrt{7}$, $Q = 1$, Modulo F_3

i	$\overline{U}_i \pmod{F_4}$	$\overline{V}_i \pmod{F_4}$
2048	9933	15934
4096	567	2016
8192	28943	960
16384	63129	4080
32768	5910	**0**
65532	5	-23
65533	6	-4
65534	1	-5
65535	1	-1
65536	**0**	-2
65537	-1	-1
65538	-1	-5
65539	-6	-4
65540	-5	-23

Table 5: $P = \sqrt{7}$, $Q = 1$, Modulo F_4

The values of $\overline{U'}_n$ and $\overline{V'}_n$ $({}_{n \geq 1})$ with $(P, Q) = (\sqrt{3}, -1)$ can be built by:

$$\begin{cases} \overline{U'}_{2n} & = & \overline{U}_{2n} \\ \overline{U'}_{2n+1} & = & \overline{V}_{2n+1} \end{cases} \qquad \begin{cases} \overline{V'}_{2n} & = & \overline{V}_{2n} \\ \overline{V'}_{2n+1} & = & \overline{U}_{2n+1} \end{cases}$$

Values of U_i and V_i in previous tables can be computed easily by the following PARI/gp programs:
U_{2j+1} : U0=1;U1=6; for(i=1,N, U0=5*U1-U0; U1=5*U0-U1; print(4*i+1," ",U0); print(4*i+1," ",U1))