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

Tony Reix (Tony.Reix@laposte.net)
2005, 14th of October

This paper provides a proof of:

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

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. (The Lehmer's theorems are also listed and detailed in my paper "A LLT-like test for proving the primality of Fermat numbers" (2004).)
Chapter 1 explains how the (P, Q) parameters have been found. Then Chapter 2 and 3 provide the proof for: M_q prime $\Longrightarrow M_q \mid S_{q-2}$ and the converse, proving theorem 1. Chapter 4 provides numerical examples. The appendix in Chapter 5 provides first values of U_n and V_n .

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

Let $S_0 = 5$ and $S_i = 2S_{i-1}^2 - 1$. $S_1 = 49$, $S_2 = 4801$, ...

It has been checked that: $\begin{cases} S_{2^n-2} \equiv 0 \pmod{M_q} & \text{for } q = 3, 5, 7, 13, 17, \ldots \\ S_{2^n-2} \not\equiv 0 \pmod{M_q} & \text{for } q = 11, 23, 29 \ldots \end{cases}$

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:

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

Thus we have: $\begin{cases} V_2 &= 2 \times S_0 &= 10 \\ V_4 &= 2 \times S_1 &= 98 \\ V_8 &= 2 \times S_2 &= 9602 \end{cases}$

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: $P = \sqrt{V_2 + 2Q} = \sqrt{12}$ or $\sqrt{8}$.
In the following we consider: $(P, Q) = (\sqrt{12}, 1)$.

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 and Q 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.

Table 1 gives values of U_i , V_i , $\overline{U}_i \pmod{M_q}$, $\overline{V}_i \pmod{M_q}$, with $(P, Q) = (\sqrt{12}, 1)$, for $q = 5$.

2 M_q prime $\Longrightarrow M_q \mid \overline{V}_{\frac{M_q-1}{2}}$ and $M_q \mid S_{q-2}$

Let $N = M_q = 2^q - 1$ with $q \geq 3$ be an odd prime.
Let: $P = \sqrt{R}$, $R = 12 = 3 \times 2^2$, $Q = 2$, and $D = P^2 - 4Q = 8 = 2^3$.

The values $\left({}^{2}\!/\!_{\mathrm{N}}\right) = 1$ and $\left({}^{3}\!/\!_{\mathrm{N}}\right) = -1$ are provided in Wiiliams' book, page 198, in the Proof of Theorem 8.4.9.

$$\text{So we have:} \quad \begin{cases} \varepsilon = \left({}^{\mathrm{D}}\!/\!_{\mathrm{N}}\right) = \left({}^{2}\!/\!_{\mathrm{N}}\right)^3 = & +1 \\ \sigma = \left({}^{\mathrm{R}}\!/\!_{\mathrm{N}}\right) = \left({}^{2}\!/\!_{\mathrm{N}}\right)^2 \left({}^{3}\!/\!_{\mathrm{N}}\right) = & -1 \\ \tau = \left({}^{\mathrm{Q}}\!/\!_{\mathrm{N}}\right) = \left({}^{1}\!/\!_{\mathrm{N}}\right) = & +1 \end{cases}$$

Since $\sigma = -\tau$ and $\sigma\epsilon = -1$, $M_q \nmid DQR$ with $q \geq 3$, then by Theorem 2 (8.4.1) we have:

$$M_q \text{ prime} \Longrightarrow M_q \mid \overline{V}_{\frac{M_q+1}{2}} = V_{2^{q-1}}$$

By (1), with $k = q - 2$, we have: $M_q \mid S_{q-2}$.

$\square$

3 $M_q \mid S_{q-2} \Longrightarrow M_q$ is a prime

Let $N = M_q$ with $q \geq 3$. By (1) we have: $N \mid S_{q-2} \Longrightarrow N \mid V_{2^{q-1}}$.
And thus, by (4.2.6) page 74 ($U_{2a} = U_a V_a$) , we have: $N \mid \overline{U}_{2^q}$.

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

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

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

□

4 Numerical Examples

(mod M_3) $S_0 = 5 \overset{1}{\mapsto} S_1 \equiv 0$
(mod M_5) $S_0 = 5 \overset{1}{\mapsto} 18 \overset{2}{\mapsto} 27 \overset{3}{\mapsto} S_3 \equiv 0$
(mod M_7) $S_0 = 5 \overset{1}{\mapsto} 49 \overset{2}{\mapsto} 102 \overset{3}{\mapsto} 106 \overset{4}{\mapsto} 119 \overset{5}{\mapsto} S_5 \equiv 0$
(mod M_{11}) $S_0 = 5 \overset{1}{\mapsto} 49 \overset{2}{\mapsto} 707 \overset{3}{\mapsto} 761 \overset{4}{\mapsto} 1686 \overset{5}{\mapsto} 672 \overset{6}{\mapsto} 440 \overset{7}{\mapsto} 316 \overset{8}{\mapsto} 1152 \overset{9}{\mapsto} S_9 \equiv 1295$

5 Appendix: Table of U_i, V_i and S_k

i	U_i		q	$\overline{U}_i\ [M_q]$	V_i		q	$\overline{V}_i\ [M_q]$	k	S_k	$S_k\ [M_q]$
0	0	$\times P$	5	0	2		5	2			
1	1		5	1	1	$\times P$	5	1			
2	1	$\times P$	5	1	10		5	10	0	5	5
3	11		5	11	9	$\times P$	5	9			
4	10	$\times P$	5	10	98		5	5	1	49	18
5	109		5	16	89	$\times P$	5	27			
6	99	$\times P$	5	6	970		5	9			
7	1079		5	25	881	$\times P$	5	13			
8	980	$\times P$	5	19	9602		5	23	2	4801	27
16	...	$\times P$	5	...	92198402		5	0	2	46099201	0

Table 1: $P = \sqrt{12}$, $Q = 1$

The values of $\overline{U'}_n$ and $\overline{V'}_n$ $(_{n\geq 1})$ with $(P,Q) = (\sqrt{8}, -1)$ 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=11; for(i=1,n, U0=10*U1-*U0; U1=10*U0-U1; print(4*i+1," ",U0); print(4*i+3," ",U1))
V_{2j} : U0=2;U1=10; for(i=1,n, U0=10*U1-*U0; U1=10*U0-U1; print(4*i," ",U0); print(4*i+2," ",U1))