A LLT-like test for Mersenne numbers, based on cycles of the Digraph under $x^2 - 2$ modulo a Mersenne prime

Tony Reix
2007, 10th of May - Updated 2008, 8th of September.
▶ Version 0.4 ◀

I'm looking for a complete proof for the following conjecture:

**Conjecture 1** $M_q = 2^q - 1$. $S_0 = 3^2 + 1/3^2$, $S_{i+1} = S_i^2 - 2 \pmod{M_q}$

$M_q$ is a prime iff $S_{q-1} \equiv S_0 \pmod{M_q}$

And we have: $\prod_{1}^{q-1} S_i \equiv 1 \pmod{M_q}$ when $M_q$ is prime

I perfectly know that this test cannot speed up the proof of primality of a Mersenne number. But the method used for proving it could be used to prove that a Mersenne is not prime faster than the classical LLT. Or it could be used for other numbers for which no LLT test does exist.

This conjecture makes use of the properties of the cycles of length $q-1$ that appear in the Digraph under $x^2 - 2$ modulo a Mersenne prime; though the LLT makes use of the properties of the tree of the same Digraph.

It has been checked with huge values of $q$.

Thanks to the help of H.C. Williams, who suggested me to use the little Fermat theorem, the first part of the conjecture has been proved.

**Now, how can we prove the converse?**

1 **Definitions**

The first part of the proof makes use of the Lucas Sequence method, as described in many papers and books, like "The Little Book of Bigger Primes" by Paulo Ribenboim or like "Édouard Lucas and Primality Testing" by Hugh C. Williams.

Hereafter, $(a \mid b)$ is the Legendre symbol.

All references to theorems apply to properties of Lucas Sequences as given by P. Ribenboim in his book "The Little Book of Bigger Primes" in 2.IV pages 44-etc.

Since $q$ is prime, we have: $M_q \equiv 1 \pmod{6q}$.

Let: $\beta = 3^2$ and $\tilde{\alpha} \equiv 1/\beta \pmod{M_q}$.

Since $M_q$ is prime, $\tilde{\alpha}$ is the only integer such that $0 < \tilde{\alpha} < M_q$. 

1
There are an infinity of $\alpha > M_q$ such that $\alpha \equiv \tilde{\alpha} \pmod{M_q}$.

Here below, we explain how to compute $\tilde{\alpha}$ and some $\alpha$.

When $q \equiv 1 \pmod{3}$ and since $q$ is odd, we have: $q \equiv 1 \pmod{6}$ . Thus $M_q = 2^q - 1 = 2^{6k+1} = 2(2^3)^{2k} - 1 \equiv 1 \pmod{9}$ . Thus $8M_q + 1 \equiv 0 \pmod{9}$ and $\tilde{\alpha} = \frac{8M_q+1}{9} \equiv 1/9 \pmod{M_q}$ .

When $q \equiv 2 \pmod{3}$ and since $q$ is odd, we have: $q \equiv 5 \pmod{6}$ . Thus $M_q = 2^q - 1 = 2^{6k+5} = 32(2^3)^{2k} - 1 \equiv 4 \pmod{9}$ . Thus $2M_q + 1 \equiv 0 \pmod{9}$ and $\tilde{\alpha} = \frac{2M_q+1}{9} \equiv 1/9 \pmod{M_q}$ .

With $q > 5$, we always have: $\beta < \tilde{\alpha} < \alpha$ .

$P = \alpha + \beta$
$Q = \alpha \beta \equiv 1 \pmod{M_q}$
$\sqrt{D} = \alpha - \beta$

And thus $\sqrt{D}$ always is a non-null positive integer.

And thus: $D = P^2 - 4Q = (\alpha - \beta)^2 \equiv P^2 - 4 \pmod{M_q}$ always is a square.

$U_n(P,Q) = U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = PU_{n-1} - QU_{n-2}$, $U_0 = 0$, $U_1 = 2$.
$V_n(P,Q) = V_n = \alpha^n + \beta^n = PV_{n-1} - QV_{n-2}$, $V_0 = 1$, $V_1 = P$.

$(D \mid M_q) = 1$ since $D$ is a square.

Let: $\alpha = \left(\frac{M_q-1}{3}\right)^2$ . It is easy to see that $\alpha \equiv 1/9 = \tilde{\alpha} \pmod{M_q}$.

If $q \equiv 1 \pmod{3}$ then $\alpha = (6k)^2$ and $\gcd(P,Q) = 9 \times \gcd((2k)^2 + 1, 9)$.
Since $x^2 \equiv 2 \pmod{9}$ has no solution, then: $\gcd(P,Q) = 9$ .

If $q \equiv 2 \pmod{3}$ then $\alpha = (1+3k)^2$ and $\gcd(P,Q) = \gcd((1+3k)^2 + 9, (1+3k)^2)$ . Since $x \mid (1+3k)^2$ and $x \mid (1+3k)^2 + 9$ only if $x = 3$ or $x = 9$ and since $3 \mid 1 + 3k$ then $\gcd(P,Q) = 1$ .

Let’s define: $S_n = V_{2^n}$.
It means: $S_{n+1} \equiv S_{n}^2 - 2 \pmod{M_q}$, $S_0 = V_2 = V_1 = P$.
So: $S_{q-1} \equiv S_0 \pmod{M_q}$ is equivalent to: $V_{\frac{M_q+1}{2}} \equiv V_1 \pmod{M_q}$ .

2 \textbf{ $M_q$ is a prime } $\Rightarrow M_q \mid S_{q-1} - S_0$

Now, let’s try to prove: $M_q$ is a prime $\Rightarrow M_q \mid V_{\frac{M_q+1}{2}} - V_1$ .

Since $M_q$ is a prime and $(D \mid M_q) = 1$, the period of $(U_n)$ and $(V_n)$ (mod $M_q$) divides $M_q - 1$ .
And thus: \( V_{Mq} \equiv V_1 \equiv P \pmod{M_q} \) and \( V_{Mq+1} \equiv V_2 \equiv P^2 - 2 \pmod{M_q} \), and \( U_{Mq} \equiv 1 \pmod{M_q} \).

By IV.2b, \( \frac{V_{Mq+1}^2}{V_2} \equiv V_{Mq+1} + 2 \equiv V_2 + 2 \equiv P^2 \equiv V_1^2 \pmod{M_q} \).

So, either we have: \( M_q | V_{Mq+1} - V_1 \) or \( M_q | V_{Mq+1} + V_1 \).

Now: \( V_{Mq-1} = \frac{\alpha Mq - 1}{2} + \frac{\beta Mq - 1}{2} \equiv (3^{Mq-1})^{-1} + 3^{Mq-1} \pmod{M_q} \).

Since \( M_q \) is a prime (and thus coprime to 3), by Fermat little theorem we have: \( 3^{Mq-1} \equiv 1 \pmod{M_q} \).

And thus: \( V_{Mq-1} \equiv 1^{-1} + 1 \equiv 2 \pmod{M_q} \).

First: since \( Q = \alpha \beta \equiv +1 \pmod{M_q} \); since \( D \equiv (-80/9)^2 \equiv (3^4-1)^2 \pmod{M_q} \); and since \( M_q \) is prime, that proves the condition of IV.23: \( M_q \not| 2QD \).

Now, by IV.23, \( \psi(M_q) = M_q - (D | M_q) = M_q - 1 \).

And then: \( U_{Mq-1} \equiv 0 \pmod{M_q} \).

Now, by IV.5b, we have: \( V_{Mq-1} = 2U_{Mq+1} - PU_{Mq-1} \).

Since \( U_{Mq-1} \equiv 0 \) and \( V_{Mq-1} \equiv 2 \pmod{M_q} \), then \( U_{Mq+1} \equiv 1 \pmod{M_q} \).

By IV.7a, we have: \( U_{Mq+1} V_1 - U_1 V_{Mq+1} \equiv 2U_{Mq-1} \pmod{M_q} \) and thus: \( V_{Mq+1} \equiv P \times 1 - 2 \times 0 \equiv P \pmod{M_q} \).

So we have: \( U_{Mq-1} \equiv 0 \), \( U_{Mq+1} \equiv 1 \), \( V_{Mq-1} \equiv 2 \), \( V_{Mq+1} \equiv P \pmod{M_q} \), proving that the period of \((U_n)\) and \((V_n)\) \( \pmod{M_q} \) equals \((M_q - 1)/2 \).

So, at the end: \( V_{Mq+1} \equiv P \equiv V_1 \pmod{M_q} \) and thus: \( M_q | V_{Mq+1} - V_1 \).

And, equivalently: \( M_q | S_{q-1} - S_0 \).

3 \( M_q \mid S_{q-1} - S_0 \Rightarrow M_q \) is a prime

And then, more difficult! How to prove the converse?

I have no idea yet ... Only some divisibility results.
4 Examples

\[
\begin{align*}
q = 5 & \quad \left\{ 
M_5 & = 31 \\
\beta & = 9 \\
\alpha & = 100 \equiv 7 \pmod{M_5} \\
P & = \alpha + \beta = 109 \equiv 16 \pmod{M_5} \\
Q & = \alpha \beta = 900 \equiv 1 \pmod{M_5} \\
gcd(P,Q) & = 1 \\
D & = P^2 - 4 = 91^2 \equiv 4 \pmod{M_5}
\end{align*}
\]

\[
\text{(mod } M_5) \quad S_0 = 16 \mapsto 6 \mapsto 3 \mapsto 7^{4=q-1} \mapsto 16
\]

\[
q = 7 & \quad \left\{ 
M_7 & = 127 \\
\beta & = 9 \\
\alpha & = 1764 \equiv 113 \pmod{M_7} \\
P & = \alpha + \beta = 1773 \equiv 122 \pmod{M_7} \\
Q & = \alpha \beta = 15876 \equiv 1 \pmod{M_7} \\
gcd(P,Q) & = 9 \\
D & = P^2 - 4 = 1755^2 \equiv 21 \pmod{M_7}
\end{align*}
\]

\[
\text{(mod } M_7) \quad S_0 = 122 \mapsto 23 \mapsto 19 \mapsto 105 \mapsto 101 \mapsto 39 \mapsto 3^{6=q-1} \mapsto 122
\]

\[
q = 13 & \quad \left\{ 
M_{13} & = 8191 \\
\beta & = 9 \\
\alpha & = 7452900 \equiv 7281 \pmod{M_{13}} \\
P & = \alpha + \beta = 7452909 \equiv 7290 \pmod{M_{13}} \\
Q & = \alpha \beta = 67076100 \equiv 1 \pmod{M_{13}} \\
gcd(P,Q) & = 9 \\
D & = P^2 - 4 = 7452891^2 \equiv 888 \pmod{M_{13}}
\end{align*}
\]

\[
\text{(mod } M_{13}) \quad S_0 = 7290 \mapsto 890 \mapsto 5762 \mapsto 2519 \mapsto 5525 \mapsto 5957 \mapsto 2435 \mapsto 7130 \mapsto 3552 \mapsto 2562 \mapsto 2851 \mapsto 2727 \mapsto 7^{12=q-1} \mapsto 7290
\]