Conjecture about a new LLT-like Primality Criterion based on Cycles of the DiGraph under $x^2 - 2$ modulo a prime used for Mersenne numbers

Tony Reix
tony.reix@laposte.net
First version: 2007, 10th of May
Updated: 2009, 21th of February and 2010, 3rd of January.
► Version 0.14 ◄

This paper presents ideas dealing with a possible new primality criterion.

The method is studied for Mersenne numbers, but it is expected that it could be used also for other numbers, like Fermat numbers, Wagstaff numbers, and others.

The main idea of the method is:
Consider a number N. Study the DiGraph under $x^2 - 2$ modulo N, which is made of Trees and Cycles. Find a Universal Seed S_0 for the family of the number, and then find a cycle such that $S_e \equiv S_s \pmod N$, with : $S_{i+1} = S_i^2 - 2 \pmod N$. Then find a Lucas sequence (U_n, V_n) that fits the S_n sequence and prove that if N is prime , then $S_e \equiv S_s \pmod N$ for some starting s and ending e values. Now, study the period $\pi(N)$ of the Lucas Sequence (U_n, V_n) and prove that the period divides $N - 1$ if and only if N is prime. This can be done by proving that, if $N = \prod f_i$, the period of $(U_n, V_n) \pmod N$ is equal to $lcm(\pi_i(f_i))$, where $\pi(f_i)$ is the period of the Lucas Sequence modulo f_i, and that $lcm(\pi_i(f_i))$ does not divide $\pi(N)$.

This **DRAFT** paper shows ideas for a proof for Mersenne numbers.
It is crystal clear that this test cannot speed up the proof of primality of a Mersenne number. However the method used for proving it (once proved !!) could be used to prove that a Mersenne is not prime faster than the classical LLT. And the same method could be used for Fermat and Wagstaff numbers.
This method 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 (the *classical* LLT makes use of the properties of the tree of the same Digraph).

I thank Dr H.C. Williams, who supported me and provided me some help when I forgot the Little Theorem of Fermat.

The fundamental ideas of this paper are based on the work of Lucas, who imagined to use the (now-called) Lucas sequences $(U_n(P,Q), V_n(P,Q))$, which are defined as (with (P,Q) integers):
$U_{n+1}(P,Q) = PU_n(P,Q) - QU_{n-1}(P,Q)$ with: $U_0(P,Q) = 0, U_1(P,Q) = 1$
$V_{n+1}(P,Q) = PV_n(P,Q) - QV_{n-1}(P,Q)$ with: $V_0(P,Q) = 2, V_1(P,Q) = P$

for proving that a number is prime, using the fastest sequence: $S_{i+1} = S_i^2 - 2 \pmod N$, with S_0 being the *seed* of the sequence.

However, it is clear that E. Lucas never imagined to use a Cycle (ending by: $S_0 \pmod N$) rather than a Tree (ending by: $0 \pmod N$) . This is the first main new idea of the test I imagined.

The second main new idea deals with the method used for trying to prove the theorem. Since the law of apparition that E. Lucas imagined does not work here ($\omega \mid \frac{N-1}{2}$ instead of $\omega \mid N-1$ as usual), I try to use the properties of the period of the Lucas Sequence, showing that the period of a non-prime number $N = \prod f_i$ is the least common multiple of the periods of the factors f_i of N, and showing that this period divides $N-1$ if and only if N is prime.

I used the books of P. Ribenboim and H.C. Williams as reference for the properties of the Lucas (U_n, V_n) sequence.
I also found some good ideas in the thesis of Dr Hinkel, who describes and proves the link between the first *apparition* of $U_n \equiv 0 \pmod N$ and the period of the (U_n, V_n) sequence.

The first part of the attempt for providing a 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.

Here after, $(a \mid b)$ or $\left(\frac{a}{b}\right)$ is the Legendre symbol.

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

Conjecture 1 (Lucas-Reix)

$$M_q = 2^q - 1 \ . \quad S_0 = 3^2 + 1/3^2, \ S_{i+1} = S_i^2 - 2 \pmod{M_q}$$
$$M_q \textit{ is a prime iff: } \ S_{q-1} \equiv S_0 \pmod{M_q}$$
$$\textit{and iff: } \ \prod_0^{q-2} S_i \equiv 1 \pmod{M_q}$$
$$\textit{and iff: } \ S_i \not\equiv S_0 \pmod{M_q}, 0 < i < q-1$$

Conjecture 2 (Reix)

$$M_q = 2^q - 1 \textit{ is a prime iff: } \ 3^{\frac{M_q-1}{2}} \equiv 1 \pmod{M_q}$$

The search for a prime should be done in two steps:

First, find PRPs by using: M_q is prime $\Rightarrow \ S_{q-1} \equiv S_0 \pmod{M_q}$.

Then, check that the number is a prime by verifying: $\prod_0^{q-2} S_i \equiv 1 \pmod{M_q}$.

1 Notations

2 General

For any N, let's call:
With $gcd(n, N) = 1$, $order(a, N)$ is the least $n > 0$ such that $a^n \equiv 1 \pmod N$.

2.1 Lucas sequence

Since we use the same Lucas sequences $(U_n(P,Q), V_n(P,Q))$ in the whole paper, it will be named as: Lucas sequences (U_n, V_n).

Instead of writing: $U_n \equiv X \pmod N$ and $V_n \equiv Y \pmod N$ for the same n and N, we will write: $(U_n, V_n) \equiv (X, Y) \pmod N$.

For any N prime, let's call:

$\omega = \omega(N)$ is the least $n > 0$ such that $U_n \equiv 0 \pmod N$.

$\Omega = \Omega(N)$ is the least $n > 0$ such that $(U_n, V_n) \equiv (0, 2) \pmod N$.

$\pi = \pi(N)$ is the least $n > 0$ such that $(U_n, V_n) \equiv (0, 2) \pmod N$ and $(U_{n+1}, V_{n+1}) \equiv (1, P) \pmod N$.

However, since, with N odd and $(U_n, V_n) \equiv (0, 2) \pmod N$, we have by IV.5b: $U_{n+1} = \frac{V_n + PU_n}{2} \equiv 1 \pmod N$ and by IV.5a: $V_{n+1} = \frac{PV_n + DU_n}{2} \equiv P \pmod N$, and thus: $(U_{n+1}, V_{n+1}) \equiv (1, P) \pmod N$.

It means that, for any (P, Q) : $\pi = \Omega$.

And we have: $(U_{\pi+i}, V_{\pi+i}) \equiv (U_i, V_i) \pmod N$ for any $i \geq 0$.

2.2 Properties of Mersenne composites

With $M_q = \prod f_i$, it is well known that:

$$\begin{cases} M_q & \equiv 1 \pmod{6q} \\ M_q & \equiv 7 \pmod{24} \\ f_i & \equiv \pm 1 \pmod 8 \\ f_i & \equiv 1 \pmod{2q} \end{cases}$$

In another paper, I've proved:

Theorem 1 (Reix) *Let $M_q = 2^q - 1$ (q prime > 3) be a Mersenne number. For each pair (a, b) of positive integers such that: $M_q = F_1 F_2$, there exist unic pairs (x, y) and (S, D) of positive integers such that:*

$$\textbf{\textit{I:}}\ M_q = (8x)^2 - (3qy)^2 \qquad \textbf{\textit{II:}}\ M_q = (1 + Sq)^2 - (Dq)^2$$

Where: $F_i = 1 + 2qA_i\ ,\ i = 1, 2$.
And:

$$\begin{cases} \mathcal{S} = & A_1 + A_2 \\ \mathcal{D} = & A_2 - A_1 \quad (A_2 > A_1) \\ \mathcal{P} = & A_1 A_2 \end{cases}$$

This entails for $\mathcal{S}$: $1 + q\mathcal{S} \equiv 0 \pmod 8$ and thus: $\mathcal{S} \equiv -q \pmod 8$ since $1/q \equiv q \pmod 8$; and for $\mathcal{D}$: $\mathcal{D}q = 3qy$ and thus: $\mathcal{D} \equiv 0 \pmod 3$.

We have: $M_q = (1 + 2qA_1)(1 + 2qA_2) = 1 + 2q(\mathcal{S} + 2q\mathcal{P}) = 1 + 6qA$.

This implies: $\mathcal{S} + 2q\mathcal{P} \equiv 0 \pmod 3$ and, since $1/q \equiv q \pmod 3$, we have: $\mathcal{P} \equiv q\mathcal{S} \pmod 3$.

$$\begin{cases} \mathcal{S} \equiv & -q & \pmod 8 \\ \mathcal{D} \equiv & 0 & \pmod 3 \\ \mathcal{P} \equiv & q\mathcal{S} & \pmod 3 \end{cases}$$

2.3 $\omega_i, \Omega_i, \pi_i$ for Mersenne composites

M_q not prime (q prime), let's call f_i the $n > 1$ prime factors of M_q: $M_q = \prod_1^n f_i$. Sometimes, we group the n factors f_i in 2 sets: $N = F_1 F_2$.

f_i prime, let's call:

$\omega_i = \omega(f_i)$ is the least $n > 0$ such that $U_n \equiv 0 \pmod{f_i}$.

$\Omega_i = \Omega(f_i)$ is the least $n > 0$ such that $(U_n, V_n) \equiv (0, 2) \pmod{f_i}$.

$\pi_i = \pi(f_i)$ is the least $n > 0$ such that $(U_n, V_n) \equiv (0, 2) \pmod{f_i}$ and $(U_{n+1}, V_{n+1}) \equiv (1, P) \pmod{f_i}$.

3 Definition of the (U_n, V_n) sequence

With q prime > 3, we have: $M_q \equiv 1 \pmod{6q}$.

Let: $\beta = 3^2$ and $\widetilde{\alpha} \equiv 1/\beta \pmod{M_q}$.
Since M_q is prime, there is only one integer $\widetilde{\alpha}$ such that $0 < \widetilde{\alpha} < M_q$.
There are an infinity of $\alpha > M_q$ such that $\alpha \equiv \widetilde{\alpha} \pmod{M_q}$.
Here below, we explain how to compute $\widetilde{\alpha}$ and some α (M_q prime or not).

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 $8M_q + 1 \equiv 0 \pmod 9 = 9\widetilde{\alpha}$ and $\widetilde{\alpha} = \frac{8M_q+1}{9} \equiv 1/9 \pmod{M_q}$.

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 $2M_q + 1 \equiv 0 \pmod 9 = 9\widetilde{\alpha}$ and $\widetilde{\alpha} = \frac{2M_q+1}{9} \equiv 1/9 \pmod{M_q}$.

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

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

$$\begin{cases} P = & \alpha + \beta \\ Q = & \alpha\beta \quad \equiv \widetilde{\alpha}\beta \equiv 1 \pmod{M_q} \\ \sqrt{D} = & \alpha - \beta \end{cases}$$

By construction, $\alpha - \beta$ is a non-null positive integer. Thus $\sqrt{D}$ always is a non-null positive integer, and $D = P^2 - 4Q \equiv P^2 - 4 \pmod{M_q}$ always is a square.
$(D \mid M_q) = 1$ since D is a square.
Since P is odd and Q is even, then by IV.18 U_n and V_n are odd, for $n \neq 0$.
By IV.25 , we have $\gcd(U_n, V_n) = 1$.

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

If $q \equiv 1 \pmod 3$ then $\alpha = (6qk)^2$ and $\gcd(P,Q) = 9 \times \gcd((2qk)^2 + 1, 9)$.
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 $3 \nmid 1 + 3k$ then $\gcd(P,Q) = 1$.

Let's define: $S_n = V_{2^n}$.

It means: $S_{n+1} \equiv S_n^2 - 2 \pmod{M_q},\ S_0 = V_{2^0} = V_1 = P$.

So: $S_{q-1} \equiv S_0 \pmod{M_q}$ is equivalent to: $V_{\frac{M_q+1}{2}} \equiv V_1 \pmod{M_q}$.

4 M_q is a prime $\implies M_q \mid S_{q-1} - S_0$

Now, lets prove: M_q is a prime $\implies M_q \mid V_{\frac{M_q+1}{2}} - V_1$.

First: since $Q = \alpha\beta \equiv +1 \pmod{M_q}$; since $D \equiv (-80/9)^2 \equiv \frac{(3^4-1)^2}{3^4} \pmod{M_q}$; and since M_q is odd prime, that proves the condition of $IV.23$: $M_q \nmid 2QD$.

Since M_q is a prime and $(D \mid M_q) = 1$, the period π of $(U_n, V_n) \pmod{M_q}$ divides $M_q - 1$, by IV.30 , $Mq \nmid 2QD$.

And thus: $V_{M_q} \equiv V_1 \equiv P \pmod{M_q}$ and $V_{M_q+1} \equiv V_2 \equiv P^2 - 2 \pmod{M_q}$, and $U_{M_q} \equiv (\frac{D}{M_q}) \equiv 1 \pmod{M_q}$, by IV.13 .

By $IV.2b$, $V^2_{\frac{M_q+1}{2}} \equiv V_{M_q+1} + 2 \equiv V_2 + 2 \equiv P^2 \equiv V_1^2 \pmod{M_q}$.

So, either we have: $M_q \mid V_{\frac{M_q+1}{2}} - V_1$ or $M_q \mid V_{\frac{M_q+1}{2}} + V_1$.

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

Since M_q is a prime (and thus coprime to 3), by Fermat little theorem we have: $3^{M_q-1} \equiv 1 \pmod{M_q}$.
And thus: $V_{\frac{M_q-1}{2}} \equiv 1^{-1} + 1 \equiv 2 \pmod{M_q}$.

Now, by *IV*.23, $\psi(M_q) = M_q - (D \mid M_q) = M_q - 1$.

And: $U_{\frac{M_q-1}{2}} \equiv 0 \pmod{M_q}$.

Now, by *IV*.5*b*, we have: $V_{\frac{M_q-1}{2}} = 2U_{\frac{M_q+1}{2}} - PU_{\frac{M_q-1}{2}}$.
Since $U_{\frac{M_q-1}{2}} \equiv 0$ and $V_{\frac{M_q-1}{2}} \equiv 2 \pmod{M_q}$, then $U_{\frac{M_q+1}{2}} \equiv 1 \pmod{M_q}$.

By *IV*.7*a*, we have: $U_{\frac{M_q+1}{2}}V_1 - U_1V_{\frac{M_q+1}{2}} \equiv 2U_{\frac{M_q-1}{2}} \pmod{M_q}$ and thus: $V_{\frac{M_q+1}{2}} \equiv 1 \times P - 2 \times 0 \equiv P \pmod{M_q}$.

So we have: $(U_{\frac{M_q-1}{2}}, V_{\frac{M_q-1}{2}}) \equiv (0, 2)$ and $(U_{\frac{M_q+1}{2}}, V_{\frac{M_q+1}{2}}) \equiv (1, P) \pmod{M_q}$, proving that the period $\pi = \pi(M_q)$ of $(U_n, V_n) \pmod{M_q}$ divides $\frac{M_q-1}{2}$!

So, at the end: $V_{\frac{M_q+1}{2}} \equiv P \equiv V_1 \pmod{M_q}$ and thus: $M_q \mid V_{\frac{M_q+1}{2}} - V_1$.
And, equivalently: $M_q \mid S_{q-1} - S_0$.

5 $\rho = order(3, M_q) = 2\pi(M_q) = 2\pi$

There is another, much shorter, way to prove the previous result.

By definition, $\rho = order(3, M_q)$ is the least n such that $3^n \equiv 1 \pmod{M_q}$.

Then, we have:

$$\begin{cases} \alpha^{\rho/2} = & (3^{-2})^{\rho/2} = & (3^{\rho})^{-1} & \equiv 1 & \pmod{M_q} \\ \beta^{\rho/2} = & (3^2)^{\rho/2} = & 3^{\rho} & \equiv 1 & \pmod{M_q} \end{cases}$$

And thus:

$$\begin{cases} U_{\rho/2} = & \frac{\alpha^{\rho/2} - \beta^{\rho/2}}{\alpha - \beta} & \equiv & 0 & \pmod{M_q} \\ V_{\rho/2} = & \alpha^{\rho/2} + \beta^{\rho/2} & \equiv & 2 & \pmod{M_q} \end{cases}$$

And, by the definition of ρ, $\rho/2$ is the least n such that $(U_n, V_n) \equiv (0, 2) \pmod{M_q}$. Which means that $\frac{\rho}{2} = \pi = \pi(M_q)$, which is the period of $(U_n, V_n) \pmod{M_q}$ as we have seen previously.

Since, when N is prime, we have: $order(a, N) \mid N - 1$, then with M_q prime: $\pi \mid \frac{M_q-1}{2}$ and π is odd since $\frac{M_q-1}{2}$.

6 ($M_q \mid S_{q-1} - S_0$ **and** $\prod_0^{q-2} S_i \equiv 1$) $\Longrightarrow$ M_q **is prime**

Now the difficult part...

6.1 $\pi \mid \frac{M_q-1}{2}$ and π is odd

($\looparrowright$ (*letter*) is a reference to the table of this section.)

Hereafter, $n = 2^{q-1}$ and $2n = 2^q$.

We have:
$$\prod_0^{q-2} S_i = \prod_0^{q-2} V_{2^i} \equiv 1 \pmod{M_q}$$

And we know: $V_{2^{q-1}} \equiv V_1 \pmod{M_q}$ $\looparrowright (a)$.

Since (IV.2a): $U_{2n} = U_n V_n$ then $U_{2^q} = U_1 V_1 V_2 V_4 ... V_{2^{q-1}} = \prod_0^{q-1} V_{2^i} \equiv 1 \times V_{2^{q-1}}$ and thus: $U_{2n} = U_{2^q} \equiv V_1 \equiv P \pmod{M_q}$ $\looparrowright (b)$.
$U_{2^q} = U_{2^{q-1}} V_{2^{q-1}} \equiv V_{2^{q-1}} \pmod{M_q}$ entails $U_n = U_{2^{q-1}} \equiv 1 \pmod{M_q}$ $\looparrowright (c)$.

Since (IV.4b): $V_{2n} = \frac{V_n^2 + DU_n^2}{2}$, then $V_{2^q} = \frac{V_{2^{q-1}}^2 + DU_{2^{q-1}}^2}{2} \equiv \frac{P^2 + (P^2-4)\times 1}{2} = P^2 - 2$ and thus $V_{2^q} \equiv V_{2^1} \pmod{M_q}$ $\looparrowright (d)$.

Since (IV.2a and IV.5b): $U_{2n} = 2U_{n+1}U_n - PU_n^2$, then $U_{n+1} = \frac{U_{2n} + PU_n^2}{2} \equiv \frac{2P}{2} \equiv P \pmod{M_q}$ $\looparrowright (e)$.

Now (IV.4a): $U_{2n+1} = U_{n+1}^2 - QU_n^2 \equiv P^2 - 1 \pmod{M_q}$ $\looparrowright (f)$.

And: $U_{2n+1} = PU_{2n} - QU_{2n-1} \equiv P^2 - U_{2n-1}$. And thus: $U_{2n-1} = U_{2^q-1} \equiv 1 \pmod{M_q}$ $\looparrowright (g)$.

Then: $U_{2n} = PU_{2n-1} - QU_{2n-2} \equiv P - U_{2n-2} = P \pmod{M_q}$.
And thus: $U_{2n-2} = U_{2^q-2} \equiv 0 \pmod{M_q}$ $\looparrowright (h)$.

By (IV.2a): $U_{2(n-1)} = U_{n-1}V_{n-1}$ and $U_{2n-2} \equiv 0 \pmod{M_q}$.
Then: $U_{n-1} = U_{2^{q-1}} \equiv 0 \pmod{M_q}$ $\looparrowright (i)$.

We have (IV.3): $U_{n+(n-1)} = V_{n-1}U_n - Q^n U_{n-(n-1)} \equiv V_{n-1}U_n - 1$.
Thus $V_{n-1} = V_{2^{q-1}} = \frac{U_{2n-1}+1}{U_n} \equiv \frac{1+1}{2} = 2 \pmod{M_q}$ $\looparrowright (j)$.

So, since we have: $(U_{n-1}, V_{n-1}) \equiv (0, 2) \pmod{M_q}$ and $(U_n, V_n) \equiv (1, P)$ then it means that, $\pi = \pi(M_q)$ being the period of the (U, V) sequence $\pmod{M_q}$, we have: $\pi \mid n - 1 = 2^{q-1} - 1 = \frac{M_q - 1}{2}$. And thus, π is odd.

Moreover, since: $1 \times M_q - 2 \times \frac{Mq-1}{2} = 1$, then $\gcd(M_q, \frac{Mq-1}{2}) = 1$.
So, since $\pi \mid \frac{Mq-1}{2}$, then $\pi \nmid M_q$.

π being the period of $(U_n, V_n) \pmod{M_q}$ means :

i	i	$U_i \pmod{M_q}$	$V_i \pmod{M_q}$
0		**0**	**2**
1		**1**	**P**
...			
$n-1$	$2^{q-1}-1$	0 $^{(i)}$	2 $^{(j)}$
n	2^{q-1}	1 $^{(c)}$	P $^{(a)}$
$n+1$	$2^{q-1}+1$	P $^{(e)}$	
...			
$2n-2$	2^q-2	0 $^{(h)}$	
$2n-1$	2^q-1	1 $^{(g)}$	
$2n$	2^q	P $^{(b)}$	P^2-2 $^{(d)}$
$2n+1$	2^q+1	P^2-2 $^{(f)}$	

Table 1: $(U_i, V_i) \pmod{M_q}$

$(U_{j\pi+i}, V_{j\pi+i}) \equiv (U_i, V_i) \pmod{M_q}$, with $i = 0...\pi-1$ and j being any positive or negative integer.

6.2 V_{2^i} are pairwise relatively prime

In P. Ribenboim's book, page 7, we have the property:
S_0 odd and $S_{n+1} = S_n^2 - 2$, then S_n are pairwise relatively prime.
Also, Bordells shown : $S_n - 2 = S_{n-2}^2 S_{n-3}^2 ... S_0^2 (S_1 - 2)$. And thus $V_{2^n} - 2 = (V_2 - 2)\prod_0^{n-2} V_{2^i}^2$ and $V_{2^n} \equiv V_2 \pmod{M_q}$.

By definition: $\alpha = (\frac{M_q - 1}{3})^2$, and we know: $M_q - 1 \equiv 0 \pmod 6$.
Thus we have : $(2q)^2 \mid \alpha$.
Since: $S_0 = V_{2^0} = P = \alpha + \beta = (2qk)^2 + 9$ then: S_0 is odd.
As a conclusion, $S_i = V_{2^i}$ are pairwise relatively prime: $\gcd(V_{2^i}, V_{2^j}) = 1$.

6.3 $\pi \nmid 2^j - 1, j = 1..q-2$

We know: $\pi \mid 2^{q-1} - 1$ and $V_{2^{q-1}} \equiv V_1 \pmod{M_q}$, and that $V_{2^{q-i}} \not\equiv V_1 \pmod{M_q}$ for $i = 2...q-1$.
Thus: $\pi \nmid 2^{q-1} - 2^{q-i} = 2^{q-i}(2^{i-1} - 1)$.
Since π is odd, then: $\pi \nmid 2^{i-1} - 1$, or: $\pi \nmid 2^j - 1, j = 1...q-2$.

6.4 $\omega = \pi$

By Hinkel 5.35 and 5.32, we have:
$(U_n, V_n) \equiv (0, 2) \pmod N \Longrightarrow \pi = \pi(N) \mid n$.
And, when $Q \equiv 1 \pmod N$, then : $\pi(N) = \omega(N)$ or $\pi(N) = 2\omega(N)$.

Now, since we have proved previously that π is odd, then: $\pi = \omega$.

6.5 *Half* period

Since we have, by IV.3a and IV.3b, : $Q^n U_{-n} = -U_n$ and $Q^n V_{-n} = V_n$ and $Q \equiv 1 \pmod{M_q}$ then: $(U_{-n}, V_{-n}) \equiv (-U_n, V_n) \pmod{M_q}$.

And, with $\pi = \pi(M_q)$ being the period of the (U_n, V_n) sequence, we have: $(U_{\pi-i}, V_{\pi-i}) \equiv (-U_i, V_i) \pmod{M_q}$, $i = 0...\lfloor \frac{\pi-1}{2} \rfloor$.

6.6 Is it Useless ?!! $\omega = \Omega = \pi$

By definition: $\omega \leq \Omega \leq \pi$.

First, let say: $\lfloor \frac{\pi-1}{2} \rfloor < \omega < \pi$.
Then: $U_{\pi-\omega} \equiv -U_\omega \equiv 0 \pmod{M_q}$ and $V_{\pi-\omega} \equiv -V_\omega \equiv 2 \pmod{M_q}$.

Thus: $\omega(M_q) = \pi - \omega < \omega$, which is a contradiction.

Now, let say: $0 < \omega \leq \pi \lfloor \frac{\pi-1}{2} \rfloor$. Thus: $2\omega < \pi$.
Then: $U_\omega \equiv 0 \pmod{M_q}$ and $U_{2\omega} \equiv U_\omega V_\omega \equiv 0 \pmod{M_q}$.

But, we know: $V_{2\omega} = \frac{V_\omega^2 + DU_\omega^2}{2} \equiv \frac{4}{2} = 2 \equiv V_\omega \pmod{M_q}$.

And: $U_{2\omega+1} = \frac{U_{2\omega}V_1 + U_1 V_{2\omega}}{2} \equiv \frac{2}{2} = 1 \pmod{M_q}$.

And: $V_{2\omega+1} = \frac{V_{2\omega}V_1 + DU_{2\omega}^2 U_1}{2} \equiv \frac{2P}{2} = P \pmod{M_q}$.
So, we have: $(U_{2\omega}, V_{2\omega}) \equiv (0, 2) \pmod{M_q}$ and $(U_{2\omega+1}, V_{2\omega+1}) \equiv (1, P) \pmod{M_q}$ which means that 2ω is also a period of (U, V) but lower than π, which is impossible.

Thus: $\omega = \pi$.

6.7 $q \mid \pi$ and $q \mid \pi_i$

How to prove that ??????????????????

6.8 $\pi \mid \frac{M_q - 1}{3^i}, i = 0, 1, 2$

How to prove that ??????????????????

6.9 Properties of $(U_n, V_n) \pmod{f_i}$

Here, $(a \mid b)$ is the Jacobi symbol.
We have: $M_q = \prod f_i = F_1 F_2$ and $(D \mid M_q) = 1 = (D \mid F_1 F_2)$.

It is well known that: $M_q \equiv -1 \pmod 8$ and $f_i \equiv \pm 1 \pmod 8$.
Thus let say: $F_1^+ \equiv +1 \pmod 8$ and: $F_2^- \equiv -1 \pmod 8$.

We have: $\frac{F_1^+ - 1}{2} \equiv 0 \pmod 4$ and $\frac{F_2^- - 1}{2} \equiv 3 \pmod 4$.

We have: $(D \mid M_q) = 1 = (D \mid F_1^+)(D \mid F_2^-)$ and:

$(D \mid F_{1,2}) = \epsilon(F_{1,2} \mid D)(-1)^{\frac{F_{1,2}-1}{2} \times \frac{D-1}{2}}$.

Since $D > 0$ and $F_{1,2} > 0$ is odd, then $\epsilon = 1$.

Since $D = (\alpha - \beta)^2$ with $\beta = 9$ and $\alpha = (\frac{M_q - 1}{3})^2 = (\frac{6qa}{3})^2 = (2qa)^2$ even, then $\alpha - \beta$ is odd, and $D = 4K + 1$. Thus: $\frac{D-1}{2} = 2K$.

$(D \mid F_1^+) = (F_1^+ \mid D)(-1)^{8kK} = (F_1^+ \mid D)$.

$(D \mid F_2^-) = (F_2^- \mid D)(-1)^{(3+4k)\times 2K} = (F_2^- \mid D)$.

The same reasonning holds when replacing F_1^+ by f_i^+ and F_2^- by f_i^- .

Now: $1 = (D \mid M_q) = (D \mid F_1^+)(D \mid F_2^-) = (F_1^+ \mid D)(F_2^- \mid D)$.

Since D is a square, we have: $(D \mid p) = (\sqrt{D} \mid p)^2 = 1$ and thus: $(D \mid F_{1,2}) = (D \mid f_i) = 1$.

6.10 $\pi_i \mid f_i - 1$

Since $M_q \nmid 2QD$ then $f_i \nmid 2QD$.
Since f_i is prime, and since we have shown that $(D \mid f_i) = 1$ and by IV.30 we have: $\pi_i = \pi(f_i)$ exists and $\pi_i \mid f_i - 1$.

6.11 $Q \equiv 1 \pmod{f_i}$

$Q = \alpha\beta \equiv 1 \pmod{M_q} \equiv 1 \pmod{\prod f_i}$.

Thus it is obvious that: $Q \equiv 1 \pmod{f_i}$ for each i .

Obvious ???? Hummmmmmmm

6.12 $\pi = lcm(\pi_i)$

Let recall:
$\pi_i = \pi(f_i)$ is the period of (U_n, V_n) modulo f_i.
$\pi = \pi(M_q)$ is the period of (U_n, V_n) modulo $M_q = \prod f_i$.

All f_i are prime and thus we have: $\gcd(\prod f_i, \prod f_j) = 1$ where $i \neq j$. Thus, we can group the divisors of M_q in two sets: F_1 and F_2 that are the product of different divisors f_i of M_q . In the (not-expected) case that there exists some f_i such that $f_i^u \mid M_q$ with $u > 1$, then all such divisors are grouped in the same set F_1 or F_2. *Hummmm Am I correct ????????????*

Let say: $m = lcm(\pi_1, \pi_2)$. We have: $m = k_1\pi_1 = k_2\pi_2$.

Thus:
$$\begin{cases} U_m = U_{k_1\pi_1} \equiv U_{\pi_1} \equiv U_0 \equiv 0 \pmod{F_1} \\ U_m = U_{k_2\pi_2} \equiv U_{\pi_2} \equiv U_0 \equiv 0 \pmod{F_2} \end{cases}$$

Since $\gcd(F_1, F_2) = 1$ then: $U_m \equiv 0 \pmod{F_1F_2}$.

Also: $\begin{cases} U_{m+1} = U_{k_1\pi_1+1} \equiv U_{\pi_1+1} \equiv U_1 \equiv 1 \pmod{F_1} \\ U_{m+1} = U_{k_2\pi_2+1} \equiv U_{\pi_2+1} \equiv U_1 \equiv 1 \pmod{F_2} \end{cases}$

Since $\gcd(F_1, F_2) = 1$ then: $U_{m+1} - 1 \equiv 0$ and thus: $U_{m+1} \equiv 1 \pmod{F_1F_2}$.

Now, since $U_{m+1} = \frac{V_mU_1+U_mV_1}{2} \equiv \frac{V_m}{2} \pmod{F_1F_2}$, thus $V_m \equiv 2 \pmod{F_1F_2}$.
And, since $V_{m+1} = \frac{V_mV_1+DU_mU_1}{2} \equiv \frac{PV_m}{2} \pmod{F_1F_2}$, thus $V_{m+1} \equiv P$.

Which shows that m is **a** period of $(U_n, V_n) \pmod{F_1F_2}$.

Now, since $m = lcm(\pi_1, \pi_2)$ is the least number that divides both π_1 and π_2, there is no number t lower than m such that t is a period of (U_n, V_n) (mod F_1F_2).

As a conclusion, the combination of each period π_i of (U_n, V_n) modulo a factor f_i of M_q implies that the period π of (U_n, V_n) modulo M_q is equal to the least common multiple of the periods π_i : $\pi = lcm(\pi_i)$.

6.13 $lcm(A_1^+, A_2^-) \nmid F_1^+F_2^- - 1$

Let say: $F_1^+ - 1 = 2qA_1^+$ and $F_2^- - 1 = 2qA_2^-$ with $F_1^+ \equiv +1 \pmod 8$ and $F_2^- \equiv -1 \pmod 8$.

Now, suppose that $lcm(A_1^+, A_2^-) \mid F_1^+F_2^- - 1 = (F_1^+ - 1)F_2^- + F_2^- - 1 = (F_2^- - 1)F_1^+ + F_1^+ - 1$.

Since we have: $A_1^+ \mid lcm(A_1^+, A_2^-)$ and $A_2^- \mid lcm(A_1^+, A_2^-)$, that implies that $A_1^+ \mid F_2^- - 1$ **and** $A_2^- \mid F_1^+ - 1$.

Now, since $F_1^+ = 1+8k_1 = 1+2qA_1^+$, we have: $qA_1^+ = 4k_1$ and thus: $A_1^+ \equiv 0 \pmod 4$ since q is odd.

Now, $A_1^+ = 4K_1$ and $F_2^- - 1 = -2 + 8K_2$ shows that $A_1^+ \nmid F_2^- - 1$.

So there is a contradiction, showing that the hypothesis ($lcm(A_1^+, A_2^-) \mid F_1^+F_2^- - 1$) is wrong.

6.14 Contradiction between: $lcm(\pi_i) = \pi$ and $\pi \mid \frac{M_q-1}{2}$

We have: $\pi_i \mid f_i - 1$ for all i and $\pi \mid \frac{M_q-1}{2} = 3qa \mid M_q - 1$.

6.15 This is the conclusion I'd like to reach !!

$\pi(f_i) \mid f_i - 1$.
$\pi = lcm(\pi_i)$.
$lcm(f_i - 1) = lcm(2qa_i)$. $lcm(a_i) \nmid \prod f_i - 1 = M_q - 1$ and $2q \mid M_q - 1$ thus $lcm(2qa_i) \nmid M_q - 1$ and $lcm(f_i - 1) \nmid M_q - 1$.

What can we conclude with $\pi_i = \pi(f_i) \mid f_i - 1$ *????????????*

$3 \mid 15 \nmid 6$ but $3 \mid 6$ .....

.....
So, if M_q is not a prime, then its period π does not divide $M_q - 1$.

6.16 Some properties..

(D. Shanks, "Solved and Unsolved... 1978": Theorem 20 page 32.)
With $f_i = 2qa_i + 1$ then:

$$\begin{cases} 3^{qa_i} \equiv +1 \pmod{f_i} & \text{iff } f_i \equiv \pm 1 \pmod{12} \\ 3^{qa_i} \equiv -1 \pmod{f_i} & \text{iff } f_i \equiv \pm 5 \pmod{12} \end{cases}$$

(W. Stein: Elementary Number Theory, 2004/11, page 73 , 4.5).
If $(a \mid p) = 1$ and if $p \equiv 3 \pmod 4$ then $a^{\frac{p+1}{4}}$ is a square root of a .

(W. Stein: Elementary Number Theory, 2004/11, page 36 , Lemma 2.5.4)
Suppose that a and b have orders r and s respectively and that $gcd(r, s) = 1$, then ab has order rs .

W. Stein: Elementary Number Theory, 2004/11, page 74, Exercise 4.2
$p \geq 5$ prime .

$$(3 \mid p) = \begin{cases} +1 & \text{iff } p \equiv \pm 1 \pmod{12} \\ -1 & \text{iff } p \equiv \pm 5 \pmod{12} \end{cases}$$

D. Burton: Elementary Number Theory, 6th Edition, Chapter 8, Problem 4 page 151.
Let say that the order of $a \pmod n$ is r and that the order of $b \pmod n$ is s, with $\gcd(r, s) = d$ and $d = \prod_{i=0}^{m} p_i^{u_i}$.
Then we have:

$$order(ab, n) = \frac{rs}{\prod_{i=0,m}^{m} p_i^{v_i}} \quad \text{with} \quad 0 \leq v_i \leq u_i \ .$$

Thus $order(ab, n) \mid rs$, and $\frac{rs}{d} \leq order(ab, n) \leq rs$.
Obviously, if $\gcd(r, s) = 1$ then $order(ab, n) = rs$.

D. Burton: Elementary Number Theory, 6th Edition, Chapter 8, Corollary of 8.1 page 149.
If a has order r modulo n, then the integers $a, a^2, ..., a^r$ are incongruent modulo n.

W. Stein: Elementary Number Theory, 2004/11, page 73
If $(a \mid p) = 1$ and if $p \equiv 3 \pmod 4$ then $a^{\frac{p+1}{4}}$ is a square root of a modulo p.

6.17 An idea...

$\pi_i \mid \frac{f_i-1}{2} = qa_i$.

Let suppose that $lcm(\pi_1, \pi_2) \mid F_1^+ F_2^- - 1$.
Then it entails: $\pi_1 \mid F_2^- - 1$ and $\pi_2 \mid F_1^+ - 1$.

We know : $F_1^+ \equiv +1 \pmod 8$ and $F_1^+ = 1 + 2qa_1$. Thus: $a_1 \equiv 0 \pmod 4$.
And: $F_2^- \equiv -1 \pmod 8$ and $F_2^- = 1 + 2qa_2$. Thus: $qa_2 \equiv -1 \pmod 4$.
Now, $\pi_1 \mid F_2^- - 1$ entails $\pi_1 \mid -1 + 4k_2$ or $\pi_1 = q$.

If π_1 is even, then this is impossible. How to prove that π_1 is even ???? as all experimental data show ! ***WRONG ! That's wrong for*** $q = 43$ ***with all combinations of*** f_1, f_2, f_3 ***! Check again !!***

By Hinkel 5.35, we have: $V_{\omega_i}^2 \equiv 4 \pmod{f_i}$.
Then: if $V_{\omega_i} \equiv 2 \pmod{f_i}$ then $\pi_i = \omega_i$.
And: if $V_{\omega_i} \equiv -2 \pmod{f_i}$ then $\pi_i = 2\omega_i$.

By Hinkel page 18: $V_n - \sqrt{D}U_n = 2\beta^n$.
With: $n = \omega_i : V_{\omega_i} \equiv 2\beta^{\omega_i} \pmod{f_i}$.
So we have to solve: $\beta^{\omega_i} \equiv \pm 1 \pmod{f_i}$.

Since $\beta = 3^2$ then: $\beta^{\omega_i} = (3^2)_i^\omega = (3_i^\omega)^2 \equiv \pm 1 \pmod{f_i}$.
Since $(-1 \mid p)_2 = 1$ when $p \equiv 1 \pmod 4$ and -1 otherwise, then $f_i \equiv 1 \pmod 8$ is a necessary condition in order to have $\pi_i = 2\omega_i$.
So, still with $f_i \equiv 1 \pmod 8$ then $x^2 \equiv -1 \pmod{f_i}$ has a solution.

How can we prove that $x = 3^\omega$ ***??***

We have the following experimental data in table 2, from q in table 3 ($-$ means -1. $+$ means $+1$):

$f_i \pmod 8$	$f_i \pmod 3$	π_i/ω_i	ρ_i/π_i	$f_i \pmod{24}$	$q \pmod 3$
$-$	$-$	1	1	23	$\pm$
$-$	$+$	1	2	7	$+$
$+$	$-$	2	2	17	$-$
$+$	$+$	2	2	1	$\pm$

Table 2: Relationships between ω_i, π_i, ρ_i for the factors f_i of M_q

6.18 Observed properties of period of Mersenne composites

When M_q has exactly 2 divisors, with π_1 and π_2 being the period of (U_n, V_n) modulo f_1 and f_2 respectiveley, let define:
$s = \pi_1 + \pi_2$, $d = \pi_2 - \pi_1$ (with $\pi_2 > \pi_1$), and $p = \pi_1\pi_2$.

Note that we have: $q \mid s$, $q \mid d$ and $q^2 \mid p$.

And we have: $1/q \equiv q \pmod 8$ and $1/q \equiv q \pmod 3$.

We observe the following properties (for $q = 11, 23, 37, 41$):

$$\begin{cases} s & \equiv & -1 & \pmod 8 \\ d & \equiv & 0 & \pmod 3 \\ p & \equiv & qs & \pmod 3 \end{cases}$$

Showing that we (should...) have:

$$\begin{cases} s/q & \equiv & \mathcal{S} & \pmod 8 \\ d/q & \equiv & \mathcal{D} & \pmod 3 \\ p & \equiv & \mathcal{P} & \pmod 3 \end{cases}$$

For $q = 11, 23, 41$ $(-1 \pmod 3)$, we have: $s = q\mathcal{S}$, $d = \mathcal{D}$, $p = q^2\mathcal{P}$.
Let call: $M = M_q$.

For $q = 37$ $(+1 \pmod 3)$, we have: $2s = q(\mathcal{S}+3)$, $2d = q(\mathcal{D}-3)$, $2p = q^2\mathcal{P}$.
Let call: $M = 2M_q - f_i$.

And it seems that: $M = (1+s)^2 - d^2 = (8x)^2 - (3qy)^2 \equiv 1 \pmod{6q}$, like M_q ...

7 Examples

$$q = 5 \quad \begin{cases} & & M_5 & = 31 & & \\ & & \beta & = 9 & & \\ & & \alpha & = 10^2 & \equiv 7 & \pmod{M_5} \\ P & = & \alpha + \beta & = 109 & \equiv 16 & \pmod{M_5} \\ Q & = & \alpha\beta & = 900 & \equiv 1 & \pmod{M_5} \\ & & \gcd(P,Q) & = 1 & & \\ D & = & P^2 - 4Q & = 91^2 & \equiv 4 & \pmod{M_5} \end{cases}$$

$\pmod{M_5}$ $S_0 = P \equiv 16 \overset{1}{\mapsto} 6 \overset{2}{\mapsto} 3 \overset{3}{\mapsto} 7 \overset{4=q-1}{\mapsto} 16$

$\prod_0^3 S_i \equiv 16 * 6 * 3 * 7 \equiv 1 \pmod{M_5}$

$$q = 7 \quad \begin{cases} & & M_7 & = 127 & & \\ & & \beta & = 9 & & \\ & & \alpha & = 42^2 & \equiv 113 & \pmod{M_7} \\ P & = & \alpha + \beta & = 1773 & \equiv 122 & \pmod{M_7} \\ Q & = & \alpha\beta & = 15876 & \equiv 1 & \pmod{M_7} \\ & & \gcd(P,Q) & = 9 & & \\ D & = & P^2 - 4Q & = 1755^2 & \equiv 21 & \pmod{M_7} \end{cases}$$

$(\text{mod } M_7)\ S_0 = P \equiv 122 \overset{1}{\mapsto} 23 \overset{2}{\mapsto} 19 \overset{3}{\mapsto} 105 \overset{4}{\mapsto} 101 \overset{5}{\mapsto} 39 \overset{6=q-1}{\mapsto} 122$

$\prod_0^5 S_i \equiv 1 \pmod{M_7}$

$$q = 11 \quad \begin{cases} & & M_{11} & = 2047 & & \\ & & \beta & = 9 & & \\ & & \alpha & = 682^2 & \equiv 455 & (\text{mod } M_{11}) \\ P & = & \alpha + \beta & = 465133 & \equiv 464 & (\text{mod } M_{11}) \\ Q & = & \alpha\beta & = 4186116 & \equiv 1 & (\text{mod } M_{11}) \\ & & \gcd(P,Q) & = 1 & & \\ D & = & P^2 - 4Q & = 465115^2 & \equiv 446 & (\text{mod } M_{11}) \end{cases}$$

$(\text{mod } M_{11})\ S_0 = P \equiv 464 \overset{1}{\mapsto} 359 \overset{2}{\mapsto} 1965 \overset{3}{\mapsto} 581 \overset{4}{\mapsto} 1851 \overset{5}{\mapsto} 1568 \overset{6}{\mapsto} 175 \overset{7}{\mapsto} 1965 \overset{8}{\mapsto} 581 \overset{9}{\mapsto} 1851 \overset{10=q-1}{\mapsto} 1568$

$\prod_0^9 S_i \equiv 1312 \pmod{M_{11}}$

$$q = 13 \quad \begin{cases} & & M_{13} & = 8191 & & \\ & & \beta & = 9 & & \\ & & \alpha & = 2730^2 & \equiv 7281 & (\text{mod } M_{13}) \\ P & = & \alpha + \beta & = 7452909 & \equiv 7290 & (\text{mod } M_{13}) \\ Q & = & \alpha\beta & = 67076100 & \equiv 1 & (\text{mod } M_{13}) \\ & & \gcd(P,Q) & = 9 & & \\ D & = & P^2 - 4Q & = 7452891^2 & \equiv 888 & (\text{mod } M_{13}) \end{cases}$$

$(\text{mod } M_{13})\ S_0 = P \equiv 7290 \overset{1}{\mapsto} 890 \overset{2}{\mapsto} 5762 \overset{3}{\mapsto} 2519 \overset{4}{\mapsto} 5525 \overset{5}{\mapsto} 5957 \overset{6}{\mapsto} 2435 \overset{7}{\mapsto} 7130 \overset{8}{\mapsto} 3552 \overset{9}{\mapsto} 2562 \overset{10}{\mapsto} 2851 \overset{11}{\mapsto} 2727 \overset{12=q-1}{\mapsto} 7290$

$\prod_0^{11} S_i \equiv 1 \pmod{M_{13}}$

8 Periods $(\text{mod } M_q)$

$M_q = 1 + 2q\alpha = \prod (1 + 2q\alpha_i)$.

In the following table (3), $\alpha_{[i]}$ is α when M_q is prime, and α_i when M_q is not prime. When M_q is not prime, $\pi/q\prod\alpha$ always is $\pi/\prod\alpha_i$. This shows that the period π depends clearly on M_q being prime or not.

Note that: 1) $q \mid \pi_q$, and: 2) π_q is odd when M_q is prime (in bold), though π_q is odd or even when M_q is not prime.

Now consider the following table (4) (for M_q prime), and compare with the column $\pi/q\prod\alpha_{[i]}$ for q of the previous table with M_q prime.

q	π	Factors of π	$(M_q-1)/\pi$	$\frac{q\prod\alpha_{[i]}}{\pi}$
5	15	$3q$	**2**	1
7	63	3^2q	**2**	1
11	44	2^2q	93/2	1
13	455	$5.7q$	**18**	**9**
17	65535	$3.5.q.257$	**2**	1
19	262143	$3^3.7.q.73$	**2**	1
23	89240	$2^3.5.q.97$	182361/1940	1
29	19836	$2^2.3^2.19.q$	3085465/114	4
31	357913941	$3.7.11.q.151.331$	**6**	**3**
37	154079544	$2^3.3.q.167.1039$	619094385/694052	6
41	13407675188	$2^2.q.59.163.8501$	2199023255551/13407675188	1
43	118642203	$3^2.q.113.2713$	22728922538/306569	5
47	165806600	$2^3.5^2.31.q.569$	1497207322929/1763900	48
53	4007499600	$2^4.3.5^2.13.37.q.131$	5664905191661/2520440	100

Table 3: Periods modulo M_q

The first part of the table has been built by computing the order $order(3, M_q)$. The second part of the table has been built by the following process: 1) Find I the greatest i such that $M_q-1 \equiv 0 \pmod{3^i}$; 2) With $n = (M_q-1)/3^i, i = 0..I$ compute $3^n \pmod{M_q}$ and find O the greatest i such that $3^n \equiv 1 \pmod{M_q}$. We see: $O \leq I$.

Based on the data in table 4, we have the conjecture:

$$\frac{M_q - 1}{order(3, M_q)} = 3^n \quad \text{with} \quad n = 0, 1, 2$$

I have been warned that the conjecture is wrong for: $q = 3217$ ***and many others.... Nuts !!!!***

$q = 3217; M_q = 2^q - 1; M_q - 1 = 3 \times \mathbf{13} \times order(3, M_q)$

9 Period $\pmod{f_i}$

Table 5.

The + or − sign before each q indicates if it is $\pm 1 \pmod 3$.
The + or − sign before each f_i indicates if it is $\pm 1 \pmod 8$.
The + or − sign after each f_i indicates if it is $\pm 1 \pmod 3$.

Notice that $\pi_i = \omega_i$ iff $f_i = -1 \pmod 8$ and $\pi_i = 2\omega$ iff $f_i = +1 \pmod 8$.

The last column in table 5 shows the relationship between the $order(3, f_i)$ and the period $\pi_i \pmod{f_i}$ of (U_n, V_n) : $\frac{order(3,f_i)}{\pi_i}$ is 1 or 2 accordingly to

q	$3^O = \frac{M_q-1}{order(3,M_q)}$	O	$I = \max i /$ $M_q - 1 \equiv 0 \pmod{3^i}$	$\frac{order(3,M_q)}{\pi}$
3	1	0	1	
5	1	0	1	2
7	1	0	2	2
13	9	2	2	2
17	1	0	1	2
19	1	0	3	2
31	3	1	2	2
61	9	2	2	
89	1	0	1	
107	1	0	1	
127	3	1	3	
521	1	0	1	
607	3	1	2	
1279	3	1	3	
2203	1	0	2	
2281	1	0	2	
3217	3	1	2	
4253	1	0	1	
4423	3	1	2	
9689	1	0	1	
9941	3	1	1	
11213	3	1	1	
19937	3	1	1	
21701	1	0	1	
23209	9	2	2	
44497	1	0	4	
86243	1	0	1	
110503	3	1	3	

Table 4: $(M_q - 1)/order(3, M_q)$.

the following conjectured relationship is:

$$order(3, f_i) = \pi_i \text{ iff: } f_i \equiv -1 \pmod 8 \text{ and } f_i \equiv -1 \pmod 3$$
$$order(3, f_i) = 2\pi_i \text{ otherwise}$$

10 Details for $q = 5$

See table 6.

11 Useful ???

And, since $F_2^- = -1 + 8k_2 = 1 + 2qA_2^-$, we have: $qA_2^- = 4k_2 - 1$.

When $q \equiv +1 \pmod 4$, then $A_2^- \equiv -1 \pmod 4$.
When $q \equiv -1 \pmod 4$, then $A_2^- \equiv +1 \pmod 4$.
And thus: $A_2^- \equiv \pm 1 \pmod 4$.

So, with $A_2^- = \pm 1 + 4K_2$ we have : $F_2^- - 1 = 2qA_2^- = 2q(\pm 1 + 4K_2) \equiv \pm - 2 \pmod 8$.

$\pm\ q$	$\pm f_i$	ω_i	π_i	π_i	$\frac{f_i-1}{\pi_i}$	$\frac{order(3,f_i)}{\pi_i}$
$-\ 11$						
	$-\ 23\ -$	11	ω	q	2	1
	$+\ 89\ -$	22	2ω	2^2q	2	2
$-\ 23$						
	$-\ 47\ -$	23	ω	q	2	1
	$+\ 178481\ -$	44620	2ω	$2^3.5.q.57$	2	2
$-\ 29$						
	$+\ 233\ -$	58	2ω	$4q$	2	2
	$-\ 1103\ -$	551	ω	$19q$	2	1
	$+\ 2089\ +$	261	2ω	2.3^2q	4	2
	$-\ f_1 \times f_2\ +$	1102	2ω	$2^2.19q$		2
	$+\ f_1 \times f_3\ -$	522	2ω	$2^2.3^2q$		2
	$-\ f_2 \times f_3\ -$	4859	2ω	$2.3^2.19q$		2
$+\ 37$						
	$-\ 223\ +$	111	ω	$3q$	2	2
	$+\ 616318177\ +$	77039772	2ω	$2^3.3.q.167.1039$	4	2
$-\ 41$						
	$-\ 13367\ -$	6683	ω	$q163$	2	1
	$+\ 164511353\ -$	41127838	2ω	$2^2q59.8501$	2	2
$+\ 43$						
	$-\ 431\ -$	43	ω	q	10	1
	$-\ 9719\ -$	4859	ω	$q113$	2	1
	$-\ 2099863\ +$	1049931	ω	3^2q2713	2	2
	$+\ f_1 \times f_2\ +$	4859	ω	$q113$		1
	$+\ f_1 \times f_3\ -$	1049931	ω	3^2q2713		2
	$+\ f_2 \times f_3\ -$	118642203	ω	$3^2q113.2713$		2
$-\ 47$						
	$-\ 2351\ -$	1175	ω	5^2q	2	1
	$+\ 4513\ +$	94	2ω	2^2q	24	2
	$+\ 13264529\ -$	3316132	2ω	$2^3.31.q.569$	2	2
	$-\ f_1 \times f_2\ -$	2350	2ω	$2^2.5^2q$		2
	$-\ f_1 \times f_3\ +$	82903300	2ω	$2^3.5^2.31q569$		2
	$+\ f_2 \times f_2\ -$					
$-\ 53$						
	$+\ 6361\ +$	795	2ω	$2.3.5q$	4	2
	$-\ 69431\ -$	34715	ω	$5q131$	2	1
	$+\ 13264529\ -$	5098600	2ω	$2^4.5^2.13.37q$	2	2

Table 5: Periods modulo f_i

i	$U_i \pmod{M_5}$	$V_i \pmod{M_5}$
0	**0**	**2**
1	**1**	**16**
2	16	6
3	7	18
4	3	3
5	10	30
6	2	12
7	22	7
8	9	7
9	29	12
10	21	30
11	28	3
12	24	18
13	15	6
14	30	16
15	**0**	**2**
16	**1**	**16**
17	16	6
18	7	18
19	3	3
20	10	30
21	2	12
22	22	7
23	9	7
24	29	12
25	21	30
26	28	3
27	24	18
28	15	6
29	30	16
30	0	2
31	1	16
32	16	6
33	7	18

Table 6: $(U_i, V_i) \pmod{M_5}$