A primality test for Fermat numbers faster than Pépin test ?

Conjecture and bits of history

Tony Reix (Tony.Reix@laposte.net)

2004, 26th of October

◦ This paper presents a conjecture that, if proven, would reduce by 25 % the time needed for proving the primality of a Fermat number.

◦ The smallest Fermat number whose primality status is unknown is: F_{33} , which is nearly 6 billions characters. A very large number. Proving it is a prime or a composite number would take years.
Proving the primality or the compositeness of Fermat numbers is done by means of a test provided by Th. Pépin in 1877. The test is simple and fast.

◦ While studying some Lucas sequence for Fermat numbers by means of the function: $x \mapsto 2x^2 - 1$, I discovered a "fixed point": the number 3 always appears at the same relative rank (2^{n-2}) in the sequence. Considering a new Lucas sequence starting from the equivalent value (6) for $x \mapsto x^2 - 2$, I found that this led to a well-known Lucas Sequence: the Pell numbers, built with $(P, Q) = (2, -1)$. After some study, it seemed possible that this Lucas sequence could provide: *if F_n divides V_{k_n}, where $k_n = 2^{3*2^{n-2}-1}$, then F_n is prime* . Proving the converse also seems possible due to numerical facts showing remarkable periods for $n = 2, 3, 4$ and not for $n = 5$, but the proof seems difficult.

◦ While I was looking for information about primality tests based on Pell numbers, I found in Williams' book that this Lucas sequence had already been studied and used by Édouard Lucas himself for providing a weaker primality test for Fermat numbers. He used a first version of this test in his book "Récréations Mathématiques".
Again in William's book appears a theorem from Emma Lehmer showing that F_n is prime if it divides $U_{(F_n-1)/16}(2, -1)$, for $n \geq 4$.

◦ Either Édouard Lucas discovered the properties I will describe hereafter in my paper but he failed to prove them and chose to provide a weaker proof, or he discovered only a sub-part. As H.C. Williams says in his book, Édouard Lucas was studying many subjects at the same time, and he may not have spent enough time to this. Also, it seems that Lucas often considered the "necessity" part of a theorem not so important ...

[In the following, R(...) refers to a theorem or property appearing in Paulo Ribenboim's book: "The Little Book of Bigger Primes" ; and W(...) refers to H.C. Williams' book: "Édouard Lucas and Primality Testing". L(...) refers to Lucas paper in the American Journal of Mathematics 1878.]

Conjecture 1 (Lucas-Reix) *Let* $n \geq 2$, $F_n = 2^{2^n} + 1$, $\mathrm{k}_n = 3 \times 2^{n-2} - 1$. F_n *is a prime* $\iff$ $F_n \mid S_{\mathrm{k}_n}$, *where:* $S_1 = 6$, $S_{i+1} = S_i^2 - 2$.

Compared to the Pépin test which requires $2^n - 1$ operations, testing only up to $3 \times 2^{n-2} - 1$ would provide a gain of 25 % in speed.

1 F_n prime $\Longrightarrow F_n \mid U_{(F_n-1)/2}(2, -1)$

Let: $N = F_n$ a prime.
We use: $x \mapsto x^2 - 2$ for building a sequence starting from 6.
We have: $S_1 = V_2 = 6, S_2 = V_4 = 34, S_3 = V_8 = 1154, \ldots \ S_i = V_{2^i}$

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

and thus: $Q = \sqrt[2]{\frac{V_2^2 - V_4}{2}} = \sqrt[4]{\frac{V_4^2 - V_8}{2}} = \pm 1$.
By W(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: $P = \sqrt{V_2 + 2Q} = 2\sqrt{2}$ or 2 , and $D = P^2 - 4Q = 4$ or 8 .

$$\begin{cases} (P, Q) = (2\sqrt{2}, +1) \ , \ D = 4 \\ \epsilon = (\mathrm{D}/\mathrm{N}) = (4/\mathrm{N}) = \ 1 \\ \sigma = (\mathrm{R}/\mathrm{N}) = (8/\mathrm{N}) = \ 1 \\ \tau = (\mathrm{Q}/\mathrm{N}) = (1/\mathrm{N}) = \ 1 \end{cases} \qquad \begin{cases} (P, Q) = (2, -1) \ , \ D = 8 \\ \epsilon = (\mathrm{D}/\mathrm{N}) = (8/\mathrm{N}) = \ 1 \\ \sigma = (\mathrm{R}/\mathrm{N}) = (4/\mathrm{N}) = \ 1 \\ \tau = (\mathrm{Q}/\mathrm{N}) = (\text{-}1/\mathrm{N}) = \ 1 \end{cases}$$

For both $Q = 1$ and $Q = -1$, by theorem W(8.4.1) page 197 , since $\sigma = \tau$, and since N is a prime, thus we have: $N \mid \overline{U}_{(N-\sigma\epsilon)/2} = \overline{U}_{(N-1)/2} = \overline{U}_{2^{2^n-1}}$, and by W(4.2.6) page 74 : $N \mid \overline{U}_{2^{2^n}}$.
Since $U_{2^n} = \prod_{i=0}^{n-1} V_{2^i}$, thus it must exist some $x \leq 2^n - 1$ such that $F_n \mid V_{2^x}$.

Hereafter, we consider $(P, Q) = (2, -1)$ (And thus: $\overline{U}n = U_n$ and $\overline{V}_n = V_n$). This Lucas Sequence builds the Pell numbers (U_n) and the companion Pell numbers (V_n), which first values are provided page 61 of Ribenboim's book.

We have: $\begin{cases} U_n = 2U_{n-1} + U_{n-2} & U_0 = 0 \quad U_1 = 1 \\ V_n = 2V_{n-1} + V_{n-2} & V_0 = 2 \quad V_1 = 2 \end{cases}$

2 Bits of history

2.1 A first theorem of Lucas about F_n numbers

In his book, H.C Williams provides a theorem from Lucas:

Theorem 1 (Lucas W(5.2.1) page 99) *Let $F_n = 2^r + 1$ ($r = 2^n$) and $T_1 = 3$. If we define the sequence $\{T_i\}$ by $T_{i+1} = 2T_i^2 - 1$, then F_n is a prime if the first term of this sequence which is divisible by F_n is T_{r-1} ... (then info about compositeness)*

I think there could be some mistakes here.

∘ Starting from: $T_1 = 3$, and with: $V_{2^i} = 2T_i$, then we have: $T_1 = 3, T_2 = 17, T_3 = 577, \ldots\ T_5 \equiv 0 \pmod{257}$. And thus F_n seems to be prime if it divides $T_{3\times 2^{n-2}-1}$. [This leads to $(P,Q) = (\sqrt{8}, 1)$ or $(P,Q) = (\sqrt{4}, -1)$, with $\epsilon = 1, \sigma = 1, \tau = 1$ in both cases. Since $\sigma = \tau$, then by Theorem W(8.4.1) page 197 we have: F_n prime $\Longrightarrow F_n \mid \overline{U}_{(F_n-\sigma\tau)/2=2^{2^n-1}}$.]

∘ Now, if we use: $T_1 = 4$ and again: $V_{2^i} = 2T_i$, then we have: $T_1 = 4, T_2 = 31, T_3 = 1921 = 17 * 113, \ldots\ T_7 \equiv 0 \pmod{257}$. And thus F_n seems to be a prime if it divides T_{r-1}. [This leads to $(P,Q) = (\sqrt{10}, 1)$ or $(P,Q) = (\sqrt{6}, -1)$, with $\epsilon = -1, \sigma = -1, \tau = 1$ in both cases. Since $\sigma = -\tau$, then by Theorem W(8.4.1) page 197 we have: F_n prime $\Longrightarrow F_n \mid \overline{V}_{(F_n-\sigma\tau)/2=2^{2^n-1}} = 2T_{2^n-1} = 2T_{r-1}$.]

So it seems the theorem should use: $T_1 = 4$.

2.2 A very interesting theorem of Lucas

Next page, H.C. Williams says that Lucas used the following theorem for proving that F_6 is composite (probably the first time a number has been proven composite without any knowledge of his factors):

Theorem 2 (Lucas W(5.2.2) page 100) *Let $F_n = 2^r + 1$ ($r = 2^n$) and $S_1 = 6 = V_2(2, -1)$. If we define the sequence $\{S_i\}$ by $S_{i+1} = S_i^2 - 2$, then F_n is a prime when $F_n \mid S_k$ for some k such that $r/2 \le k \le r-1$. Also, F_n is composite if $F_n \nmid S_k$ for all $k \le r-1$. Finally, if $F_n \mid S_k$ with $k \le r/2$, then any prime divisor of F_n must have the form $2^{k+1}q + 1$.*

This test is sufficient for proving the primality of a Fermat number, but it is not necessary.
H.C. Williams does not provide the proof. Rather, he says that "by using the same reasoning as that employed in the proof of Theorem (5.1.2) the result follows easily". Since this proof deals with Mersenne numbers and is based on the facts that $M_n \mid U_{M_\alpha+1}$ and $M_n \nmid U_{(M_\alpha+1)/2}$ in order to say that the rank of apparition ω (the least value of m such that $m \mid U_n$) of a prime divisor of M_n is 2^α, probably based on theorem W(4.3.13) page 90,

and since we have seen previously that $F_n \mid \overline{U}_{2^{2^n-1}}$ and $F_n \mid \overline{U}_{2^{2^n}}$, there is something I don't understand.

The original text from Lucas is really not clear, even for a French reader. Lucas says that this theorem is a direct consequence of his "fundamental theorem" and of the duplication formulae, with no complementary explanation. I propose here another translation:

Theorem 3 (Lucas L(XXVIII) page 313) *Let $F_n = 2^{2^n} + 1$; we create the sequence of the $2^n - 1$ numbers: $6, 34, 1154, 13\ 31714, 17\ 73462\ 17794, \ldots$, so that each of them is equal to the square of the previous one minus 2. The number F_n is a prime when the first element of the sequence which is divisible by F_n appears between rank 2^{n-1} and rank $2^n - 1$; it is a composite number if no element of the sequence is divisible by F_n. Finally, if $\alpha < 2^{n-1}$ is the rank of the first element of the sequence which is divisible by F_n, the prime divisors of F_n have the form: $2^{2^{n+1}}q + 1$.*

Then Lucas says that Father Pépin's method is appropriate for proving that a Fermat number is prime. But, since (according to Father Mersenne) Fermat numbers F_n with $n > 4$ seem to be all composite, instead of knowing if the Fermat number is prime or not when the last operation is done by means of Pépin's test, it would be more efficient to *use one of the* $\phi(2^{n-1})$ *numbers that belong to exponent* 2^{n-1} (not clear for me ...) .
(It is clear that a clear proof for Lucas' theorem would be really useful.)
I also suspect that errors may have been added to the original manuscript and that Lucas did not fixed them all before it was published.

2.3 F_6 in "Récréations Mathématiques"

In his book: "Récréations Mathématiques", published in 1891, page 235, Édouard Lucas says that, starting with $S_0 = 6$ and using: $S_{i+1} = S_i^2 - 2$, F_n is prime if $F_n \mid S_{2^n-1}$. He also says that he used this for proving that $F_6 = 2^{64} + 1$ is composite. So $2^n - 1 = 63$ operations were required.

2.4 A hint from Édouard Lucas

In his book, page 108, H.C. Williams' provides comments from Édouard Lucas about his method. The most interesting information is that Lucas explains that his *procedure* is able to prove the primality of F_2, F_3, F_4 "by executing respectively 3, 6, or 12 operations instead of the maximum number of 4, 8 and 16 operations which would be required by the other method".

These numbers of operations: 3, 6, and 12 are equal to the value of k_n for $n = 2, 3, 4$, plus 1 :

$$\mathrm{k}_2 = 3 \times 2^0 - 1 = 2\ , \quad \mathrm{k}_3 = 3 \times 2^1 - 1 = 5\ , \quad \mathrm{k}_4 = 3 \times 2^2 - 1 = 11.$$

2.5 A Theorem from Emma Lehmer

Page 108 and 109 of his book, Williams provides a theorem of Emma Lehmer that can be used for proving the primality of Fermat numbers. It requires 4 steps less than Pépin's test when $n \geq 4$. Maybe it is a first step in the direction of a proof of our conjecture, since $\frac{F_4-1}{16} = 4096 = 2k_4$.

Theorem 4 (E. Lehmer W(5.4.1) page 108) *If p is a prime such that $p \equiv 1 \pmod{32}$ and $p = a^2 + 64b^2 = c^2 + 128d^2 \quad (a, b, c, d \in \mathbb{Z})$, then $U_{(p-1)/16}(2, -1) \equiv 0 \pmod{p}$ if and only if $b \equiv d \pmod{2}$.*

Since $F_n = (2^{2^{n-1}})^2 + 1 = (2^{2^{n-1}} - 1)^2 + 2(2^{2^{n-2}})^2$, thus, if $n \geq 4$ and F_n is a prime, we must have: $U_{(F_n-1)/16}(2, -1) \equiv 0 (\bmod\ F_n)$. It follows that if F_n is a prime, then $F_n \mid S_t$, where $t \leq r - 5$ $(n \geq 4)$.

3 Computed properties of Pell numbers $(\bmod\ F_n)$

3.1 Pell numbers $(\bmod\ F_2)$

i	U_n	$U_n[F_2]$	V_n	$V_n[F_2]$	i	U_n	$U_n[F_2]$	V_n	$V_n[F_2]$
0	0	**0**	2	2	8	408	**0**	1154	15
1	1	1	2	2	9	985	16	2786	15
2	2	2	6	6	10	2378	15	6726	11
3	5	5	14	14	11	5741	12	16238	3
4	12	12	34	**0**	12	13860	5	39202	**0**
5	29	12	82	14	13	33461	5	94642	3
6	70	2	198	11	14	80782	15	228486	6
7	169	16	478	2	15	195025	1	551614	15
16	470832	**0**	1331714	2					
17	1136689	1	3215042	2					
...									

Table 1: F_2

It appears clearly that there is a period of $16 = F_2 - 1$ amongst the values of U_i and V_i modulo F_2. As seen later, the period $F_n - 1$ amongst the U_i and V_i sequences can be easily proven for all primes, not only for Fermat numbers. Also, we have the following symmetries:

$$U_{8+i} \equiv -U_i \ , \ V_{8+i} \equiv -V_i \ , \ U_{8+i}V_{8+i} \equiv U_iV_i \quad \text{for } i = 0...7.$$

$$U_{4j+i} \equiv (-1)^{i+j-1}U_{4j-i} \ , \ V_{4j+i} \equiv (-1)^{i+j}V_{4j-i} \quad \text{for } i, j = 1...4.$$

Examples:

$U_9 \equiv -U_1$, $V_{15} \equiv -V_7$, $U_1V_2 \equiv U_{10}V_{10} \equiv 12$.
$U_5 \equiv -U_3$, $U_6 \equiv U_2$, $V_5 \equiv V_3$, $V_6 \equiv -V_2$.

Also notice: $U_2 \equiv 2^1$, $V_2 \equiv 2^3 - 2^1$, $U_4 \equiv 2^3 + 2^2 \pmod{F_2}$.

3.2 Pell numbers $\pmod{F_3}$

i	$U_n[F_3]$	$V_n[F_3]$	i	$U_n[F_3]$	$V_n[F_3]$
0	**0**	2	64	**0**	255
1	1	2	65	256	255
2	2	6	66	255	251
3	5	14	67	252	243
4	12	34	68	245	223
...					
8	151	126	72	106	131
...					
16	8	197	80	249	60
...					
24	86	24	88	171	233
...					
31	223	136	95	34	121
32	34	**0**	96	223	**0**
33	34	136	97	223	121
...					
40	86	233	104	171	24
...					
48	8	60	112	249	197
...					
56	151	131	120	106	126
...					
60	12	223	124	245	34
61	252	14	125	5	243
62	2	251	126	255	6
63	256	2	127	1	255
128	**0**	2			
129	1	2			

Table 2: F_3

Now, the period is: $128 = (F_3-1)/2$. No general property of Lucas sequence exists for proving this period. A specific property must be built for this case. We find for F_3 the same kind of symmetries we had for F_2 :

$$U_{64+i} \equiv -U_i \ , \ V_{64+i} \equiv -V_i \ , \ U_{64+i}V_{64+i} \equiv U_iV_i \quad \text{for } i = 0...63.$$

$$U_{32j+i} \equiv (-1)^{i+j-1}U_{32j-i} \ , \ V_{32j+i} \equiv (-1)^{i+j}V_{32j-i} \quad \text{for } i,j = 1...32.$$

Examples:

$U_{65} \equiv -U_1$, $V_{120} \equiv -V_{56}$, $U_{60}V_{60} \equiv U_{124}V_{124} \equiv 106$.
$U_{33} \equiv -U_{31}$, $U_{48} \equiv U_{16}$, $V_{61} \equiv V_3$, $V_{48} \equiv -V_{16}$.

Also notice: $U_{16} \equiv 2^3$, $V_{16} \equiv -(2^6-2^2)$, $V_{31} \equiv 2^3F_2$, $U_{32} \equiv 2^5+2^1 \equiv 2^1F_2$.

3.3 Pell numbers (mod F_4)

i	$U_n[F_4]$	$V_n[F_4]$	i	$U_n[F_4]$	$V_n[F_4]$
0	**0**	2	4096	**0**	65535
1	1	2	4097	65536	65535
2	2	6	4098	65535	65531
3	5	14	4099	65532	65523
4	12	34	4100	65525	65503
...					
1024	65409	4080	5120	128	61457
...					
2046	6168	49089	6142	59369	16448
2047	63481	8224	6143	2056	57313
2048	2056	**0**	6144	63481	**0**
2049	2056	8224	6145	63481	57313
2050	6168	16448	6146	59369	49089
...					
3072	65409	61457	7168	128	4080
...					
4092	12	65503	8188	65525	34
4093	65532	14	8189	5	65523
4094	2	65531	8190	65535	6
4095	65536	2	8191	1	65535
8192	**0**	2			
8193	1	2			

Table 3: F_4

Now, the period is: $8192 = (F_4 - 1)/8$.
We find for F_4 the same kind of symmetries we had for F_2 and F_3.

Also notice: $U_{1024} \equiv -2^7$, $V_{1024} \equiv 2^{12} - 2^4$, $U_{2046} \equiv 24F_3$, $V_{2046} \equiv -2^6F_3$, $U_{2047} \equiv -2^3F_3$, $V_{2047} \equiv 2^5F_3$, $U_{2048} \equiv 2^{11} + 2^3 \equiv 2^3F_3$ (mod F_4).

3.4 Pell numbers (mod F_5)

i	$U_n[F_5]$	$V_n[F_5]$	i	$U_n[F_5]$	$V_n[F_5]$
0	**0**	2	5583680	**0**	4294967295
1	1	2	5583681	4294967296	4294967295
2	2	6	5583682	4294967295	4294967291
3	5	14	5583683	4294967292	4294967283
4	12	34	5583684	4294967285	4294967263
...					
1395920	4294934529	16776960	6979600	32768	4278190337
...					
2791837	4236246145	167774720	8375517	58721152	4127192577
2791838	25166208	4227857409	8375518	4269801089	67109888
2791839	4286578561	33554944	8375519	8388736	4261412353
2791840	8388736	**0**	8375520	4286578561	**0**
2791841	8388736	33554944	8375521	4286578561	4261412353
2791842	25166208	67109888	8375522	4269801089	4227857409
2791843	58721152	167774720	8375523	4236246145	4127192577
...					
5583676	12	4294967263	11167356	4294967285	34
5583677	4294967292	14	11167357	5	4294967283
5583678	2	4294967291	11167358	4294967295	6
5583679	4294967296	2	11167359	1	4294967295
11167360	**0**	2			
11167361	1	2			

Table 4: F_5

Here, the period is: $11167360 = 2^7 \times 5 \times 17449$.
Since: $F_5 = f_1 \times f_2$ and $f_1 = 641 = 1 + 5 \times 2^7$, $f_2 = 6700417 = 1 + 3 \times 17449 \times 2^7$, it appears that the period is equal to: $((f_1 - 1)(f_2 - 1))/(3 \times 2^7)$.

We also observe the same symmetries we saw with F_n , for $n = 2, 3, 4$.

Also notice: $U_{2791840/2} \equiv -2^{15}$, $V_{2791840/2} \equiv 2^8 \times F_0 \times F_1 \times F_2 \times F_3$, $U_{2791838} \equiv 3 \times 2^7 F_4$, $V_{2791838} \equiv 2^{10} F_4$, $U_{2791839} \equiv -2^7 F_4$, $V_{2791839} \equiv 2^9 F_4$, $U_{2791840} \equiv 2^{23} + 2^7 \equiv 2^7 F_4 \pmod{F_5}$.

3.5 General Properties of Pell numbers (mod F_n)

With F_n prime, we clearly see that we have the following properties:

• Period of $(U_i, V_i) \pmod{F_n}$:
Let call: $\mathrm{P_n}$ the period of $(U_i, V_i) \pmod{F_n}$.

Let call: $\mathrm{p_n} = 3 \times 2^{n-2} + 1$.
We have: $\mathrm{P_n} = 2^{\mathrm{p_n}}$ and $\mathrm{k_n} = \mathrm{p_n} - 2$.

- Values of i such that $F_n \mid U_i$ or $F_n \mid V_i$:

We have: $F_n \mid U_i$ for $i = \frac{\alpha}{2}\mathrm{P_n}$, and $F_n \mid V_i$ for $i = \frac{4\alpha\pm1}{4}\mathrm{P_n}$, $\alpha = 0, 1, \ldots$.

$$\text{Let call:} \begin{cases} I_U \text{ the values of } i \text{ such that } F_n \mid U_i \\ I_V \text{ the values of } i \text{ such that } F_n \mid V_i \end{cases}$$

- We have the following symmetries :

$$\begin{cases} U_{I_U+\beta} \equiv (-1)^{\beta-1} U_{I_U-\beta} \\ V_{I_V+\beta} \equiv (-1)^{\beta-1} V_{I_V-\beta} \\ U_{I_V+\beta} \equiv (-1)^{\beta} U_{I_V-\beta} \\ V_{I_U+\beta} \equiv (-1)^{\beta} V_{I_U-\beta} \end{cases}$$

n	F_n	I_U	I_V	period $\mathrm{P_n}$
2	2^4+1	$8 = 2^3$ $16 = 2^4$	$4 = 2^2$ $12 = 3 \times 2^4$	2^4
3	2^8+1	$64 = 2^6$ $128 = 2^7$ ...	$32 = 2^5$ $96 = 3 \times 2^5$ ...	2^7
4	$2^{16}+1$	$4096 = 2^{12}$ $8192 = 2^{13}$ ...	$2048 = 2^{11}$ $6144 = 3 \times 2^{11}$ ...	2^{13}
5	$2^{32}+1$	5583680 11167360	2791840 8375520	11167360

Table 5: Period of Pell Sequence modulo a Fermat number

n	F_n	$\overline{U}_{(F_n-1)/2}$	$V_2^{3\times2^{n-2}-1}$
2	2^4+1	U_{2^3}	V_{2^2}
3	2^8+1	U_{2^7}	V_{2^5}
4	$2^{16}+1$	$U_{2^{15}}$	$V_{2^{11}}$
5	$2^{32}+1$	$U_{2^{31}}$	$V_{2^{23}}$

Table 6: $V_{2^{\mathrm{k_n}}}$

3.6 Pell numbers $(\mathrm{mod}\ 2^i)$

For numbers 2^i, $U_j \equiv 0 \pmod{2^i}$ for $j = 2^i$ and the period is 2^i . There is no j such that $V_j \equiv 0 \pmod{2^i}$.

3.7 Pell numbers (mod a prime number)

Here we provide information about the Pell sequence modulo different prime numbers. All these numbers share the symmetry properties around the ranks for which $U_i \equiv 0$ and $V_i \equiv 0$: I_U and I_V.

p	I_U	I_V	period	
5	3 , 6 , 9 , 12		12	$2(p+1)$
7	6	3	6	$p-1$
11	12 , 24	6 , 18	24	$2(p+1)$
13	7 , 14 , 21 , 28		28	$2(p+1)$
17	8 , 16	4 , 12	16	$p-1$
19	20 , 40	10 , 30	40	$2(p+1)$
23	22	11	22	$p-1$
29	10 , 20		20	$2/3(p+1)$
31	30	15	30	$p-1$
37	19 , 38 , 57 , 76		76	$2(p+1)$
41	10	5	10	$(p-1)/4$
43	44 , 88	22 , 66	88	$2(p+1)$
47	46	23	46	$p-1$
53	27 , 54 , 81 , 108		108	$2(p+1)$
59	20 , 40	10 , 30	40	$2/3(p+1)$
61	31 , 62 , 93 , 124		124	$2(p+1)$
67	68 , 136	34 , 102	136	$2(p+1)$
71	70	35	70	$p-1$
73	36 , 72	18 , 54	72	$p-1$
79	26	13	26	$(p-1)/3$

Table 7: Periods of Pell Sequence modulo a Prime

3.8 Pell numbers (mod a Mersenne number)

Here we provide information about the Pell sequence modulo several Mersenne numbers (prime or not). All these numbers share the symmetry properties around the ranks for which $U_i \equiv 0$ and $V_i \equiv 0$: I_U and I_V.
They mainly differ by the **main period** (when the sequence of residues restarts from begining) and by **secondary periods** (the number of time the element is congruent to 0).
It appears that the main period divides $M_q - 1$ for Mersenne primes (like for Fermat primes) but with no apparent rule.
About secondary periods, Mersenne primes seem to have only one secondary period, compared to the 2 secondary periods for Fermat primes.

p	I_U	I_V	period	
2^3-1	6	3	6	$= 2.3 = 2^3-2$
2^4-1	12 , 24		24	$= 2^3.3$
2^5-1	30	15	30	$= 2.3.5 = 2^5-2$
2^6-1	12 , 24		24	$= 2^3.3$
2^7-1	126	63	126	$= 2.3^2.7 = 2^7-2$
2^8-1	24 , 48		48	$= 2^4.3$
2^9-1	36 , 72		72	$= 2^3.3^2$
$2^{10}-1$	60 , 120		120	$= 2^3.3.5$
$2^{11}-1$	44 , 88		88	$= 2^3.11$
$2^{12}-1$	84 , 168		168	$= 2^3.3.7$
$2^{13}-1$	630	315	630	$= 2.3^2.5.91 = (2^{13}-2)/13$
$2^{14}-1$	2772 , 5544		5544	$= 2^3.3^2.7.11$
$2^{15}-1$	150	75	150	$= 2.3.5^2$
$2^{16}-1$	192 , 384		384	$= 2^7.3$
$2^{17}-1$	131070	65535	131070	$= 2.3.5.17.257 = 2^{17}-2$
$2^{18}-1$	180 , 360		360	$= 2^3.3^2.5$
$2^{19}-1$	74898	37449	74898	$= 2.3^3.19.73 = (2^{19}-2)/7$
$2^{20}-1$	60 , 120		120	$= 2^3.3.5$
$2^{21}-1$	252 , 1504		1504	$= 2^3.3^2.7$
$2^{22}-1$	2508 , 5016		5016	$= 2^3.3.11.19$
$2^{23}-1$	4462 , 8924		8924	$= 2^2.23.97$
$2^{24}-1$	840 , 1680		1680	$= 2^4.3.5.7$
$2^{25}-1$	900 , 1800		1800	$= 2^3.3^2.5^2$
$2^{26}-1$	860580 , 1721160		1721160	$= 2^3.3^2.5.7.683$
$2^{27}-1$	65664 , 131328		131328	$= 2^8.3^3.19$
$2^{28}-1$	13860 , 27720		27720	$= 2^3.3^2.5.7.11$
$2^{29}-1$	6612 , 13224		13224	$= 2^3.3.19.29$
$2^{30}-1$	24900 , 49800		49800	$= 2^3.3.5^2.83$
$2^{31}-1$	1099582	549791	1099582	$= (2^{31}-2)/(3^2.7.31)$
$2^{32}-1$	12288 , 24576		24576	$= 2^{13}.3$
$2^{33}-1$	1198956 , 2397912		2397912	$= 2^3.3.11.31.293$
$2^{34}-1$	86768340 , 173536680		173536680	$= 2^3.3.5.17.257.331$
$2^{35}-1$	553140 , 1106280		1106280	$= 2^3.3^2.5.7.439$
$2^{36}-1$	263340 , 526680		526680	$= 2^3.3^2.5.7.11.19$

Table 8: Periods of Pell Sequence modulo M_q

p	I_U	I_V	period	
6	4 , 8	2 , 6	8	
8	8		8	
9	12 , 24	6 , 18	24	
10	6 , 12		12	
12	4 , 8		8	
14	6	3	6	
15	12 , 24		24	
16	16		16	
18	12 , 24	6 18	24	
20	12		12	
21	12 , 24		24	
22	12 , 24	6 , 18	24	
24	8		8	
25	15 , 30 , 45 , 60		60	
26	14 28		28	
27	36, 72	18 , 54	72	
28	12		12	
30	12 , 24		24	
32	32		32	
33	12 , 24	6 , 18	24	
34	8 , 16	4 , 12	16	
35	6 , 12		12	
36	12 , 24		24	
38	20 , 40	10 , 30	40	
39	28 , 56		56	
40	24		24	
42	12 , 24		24	
44	12 , 24		24	
45	12 , 24		24	
46	22	11	22	
48	16		16	
49	42	21	42	
50	30 , 60		60	
51	8 , 16		16	
52	28		28	
54	36 , 72	18 , 54	72	
55	12 , 24		24	

Table 9: Periods of Pell Sequence modulo a Composite

3.9 Pell numbers (mod a composite number)

3.10 Conclusion of Pell numbers (mod N)

It appears that the main difference between Fermat primes and other numbers is the period (lower than the modulo) and the 2 sub-periods.

4 Properties of Pell numbers

4.1 Proven Properties

Here are several properties of Pell numbers, derived from Ribenboim's or Williams' books:

- By W(4.2.29) page 77, we have:

$$V_n = 2\sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} 2^i$$

- By R(IV.8) page 47, we have:

$$V_{2^j} = 2\sum_{i=0}^{2^{j-1}} \binom{2^j}{2i} 2^i$$

- By W(4.2.29) page 77, we have:

$$U_n = \sum_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n}{2i+1} 2^i$$

- Another formula from Rajesh Ram:

$$U_n = 2\sum_{i=1}^{\lfloor \frac{n+1}{2} \rfloor} \binom{n-i}{i-1} 2^{n-2i}$$

- By R(IV.14) page 49 :

$$F_n \text{ prime } \Longrightarrow V_{F_n} \equiv P = 2 \pmod{F_n}$$

- By R(IV.13) page 49 , we have:

$$F_n \text{ prime } \Longrightarrow U_{F_n} \equiv 1 \pmod{F_n}$$

- By R(IV.22) page 53, we have:

$$F_n \nmid 2QD \text{ and } F_n \text{ prime } \Longrightarrow V_{F_n-1} \equiv 2 \pmod{F_n}$$

- By R(IV.30) page 55, we have the **general period** property:

$$p \nmid 2QD, (\mathrm{D}/\mathrm{p}) = 1 \Longrightarrow \begin{cases} U_{n+p-1} \mid U_n \pmod{p} \\ V_{n+p-1} \mid V_n \pmod{p} \end{cases}$$

• The minimum polynomial for: $\sin 2\pi/p$ is:

$$S_p(x) = \sum_{i=0}^{(p-1)/2} (-1)^i \binom{p}{2i+1} (1-x^2)^{(p-1)/2-i} x^{2i}$$

$$S_p(\sqrt{2}) = (-1)^{(p-1)/2} \sum_{i=0}^{\frac{p-1}{2}} \binom{p}{2i+1} 2^i \text{ and } S_p(\sqrt{2}) = U_p(2,-1) \text{ for } p \text{ odd}$$

5 Unproven Properties $\pmod{F_n}$

Here are collected a list of properties verified by the $U_n(2,-1)$ and $V_n(2,-1)$ Lucas sequences, for $n = 2, 3, 4$.

$$V_n = 2(U_n + U_{n-1})$$

$$V_n = 2 + 4 \sum_{i=1}^{n-1} U_i$$

$$V_i^2 + V_{i+1}^2 = V_{2i} + V_{2(i+1)}$$

$$U_{pk+q} \equiv (-1)^{q-1} U_{pk-q} \pmod{F_n} \text{ with: } k = 2^{3\times 2^{n-2}-1}, p = 1..., q = 1...$$

$$U_{p\pm k} \equiv \frac{1}{2} U_k V_p \text{ with: } k = 2^{3\times 2^{n-2}-1}$$

$$\text{Let: } \alpha_n = 2^{2^{n-2}} \prod_{i=0}^{n-2} F_i = (F_{n-2} - 1)(F_{n-1} - 2)$$

$$\text{we have: } \alpha_n^2 - 2 \equiv 0 \pmod{F_n}$$

6 Conclusions

Though it is clear that Édouard Lucas had made numerical experiments with his $S_n = S_{n-1}^2 - 2$ sequence starting with $S_0 = 6$, it seems that he did not study in details the period of the Pell Sequence modulo a Fermat number or modulo another number.
Otherwise, I think he would have given this information.

What is needed for proving the conjecture ?

⋆ First, a clear proof of: F_n *is a prime* $\Longleftrightarrow F_n \mid U_{F_{(n-1)/2}}(2,-1)$ must be built. Then it will be immediate to show: $F_n \mid S_{\mathrm{k}n} \implies F_n$ *is a prime.*

⋆ Second, a proof of the results we saw about the period of the Pell sequences $(2,-1)$ modulo a Fermat prime must be built. Then it will be immediate to show: F_n *is a prime* $\Longrightarrow F_n \mid S_{\mathrm{k}n}$.

7 Miscellaneous Properties of Lucas Sequences

- By W(4.2.27) page 76, we have:

$$V_pV_q = U_{p+q} - (-1)^q U_{p-q}$$

- By W(4.2.6) page 74, we have:

$$U_{2^n} = \prod_{i=0}^{n-1} V_{2^i}$$

- By R(IV.10) page 48, we have:

$$U_n = Q^{(n-1)/2} + \sum_{i=0}^{(n-3)/2} Q^i V_{n-(2i+1)} \text{ , } n \text{ odd}$$

- By the binomial formula:

$$(1+2)^n = \sum_{i=0}^{n} \binom{n}{i} 2^i = 3^n$$

- By ???, we have:

$$[\sum_{i=0}^{n} \binom{n}{i} x^i]^2 = \sum_{i=0}^{n} \binom{2n}{2i} x^{2i}$$

- By ???, we have:

$$[\sum_{i=0}^{n} \binom{n}{i} x^i]^2 \times [\sum_{i=0}^{n} (-1)^i \binom{n}{i} x^i]^2 = \sum_{i=0}^{n} (-1)^i \binom{n}{i} x^{2i}$$