Properties of Pell numbers modulo prime Fermat numbers

Tony Reix (Tony.Reix@laposte.net)
2005, ??th of February

The Pell numbers are generated by the Lucas Sequence:
$X_n = PX_{n-1} - QX_{n-2}$ with $(P,Q) = (2,-1)$ and $D = P^2 - 4Q = 8$.
There are:
◦ The Pell Sequence: $U_n = 2U_{n-1} + U_{n-2}$ with $(U_0, U_1) = (0, 1)$, and
◦ The Companion Pell Sequence: $V_n = 2V_{n-1} + V_{n-2}$ with $(V_0, V_1) = (2, 2)$.

The properties of Lucas Sequences (named from Édouard Lucas) are studied since hundreds of years. Paulo Ribenboim and H.C. Williams provided the properties of Lucas Sequences in their 2 famous books: "The Little Book of Bigger Primes" (PR) and "Édouard Lucas and Primality Testing" (HCW).

The goal of this paper is to gather all known properties of Pell numbers in order to try proving a faster Primality test of Fermat numbers. Though these properties are detailed in the Ribenboim's and Williams' books, the special values of (P,Q) lead to new properties.

Properties from Ribenboim's book are noted: (PR).
Properties from Williams' book are noted: (HCW).
Properties built by myself are noted: (TR).

n	-3	-2	-1	0	1	2	3	4	5	6	7	8	9	10
U_n	5	-2	1	0	1	2	5	12	29	70	169	408	985	2378
V_n	-14	6	-2	2	2	6	14	34	82	198	478	1154	2786	6726

Table 1: First Pell numbers

1 General properties of Pell numbers

1.1 The Little Book of Bigger Primes

The polynomial $X^2 - 2X - 1$ has discriminant $D = 8$ and roots:

$$\left.\begin{matrix}\alpha\\ \beta\end{matrix}\right\} = 1 \pm \sqrt{2}$$

So:

$$\begin{cases} \alpha+\beta &= 2 \\ \alpha\beta &= -1 \\ \alpha-\beta &= 2\sqrt{2} \end{cases}$$

and we define the sequences of numbers:

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad V_n = \alpha^n + \beta^n \quad \text{for } n \geq 0.$$

Hereafter, n and m represent any positive or negative integer.
p represents a prime number.

The properties provided by P. Ribenboim have been extended for negative values of n of U_n and V_n :

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

(PR) IV.1 $U_n = 2U_{n-1} + U_{n-2} \quad U_0 = 0, U_1 = 1$
$V_n = 2V_{n-1} + V_{n-2} \quad V_0 = 2, V_1 = 2$

(PR) IV.2 $U_{2n} = U_n V_n$
$V_{2n} = V_n^2 - 2(-1)^n$

(PR) IV.3 $U_{m+n} = U_m V_n - (-1)^n U_{m-n}$
$V_{m+n} = V_m V_n - (-1)^n V_{m-n}$

(PR) IV.4 $U_{m+n} = U_m U_{n+1} + U_{m-1} U_n$
$2V_{m+n} = V_m V_n + 8U_m U_n$

(PR) IV.5 $4U_n = V_{n+1} - V_n$
$4U_n = V_n + V_{n-1}$
$8U_n = V_{n+1} + V_{n-1}$

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

(PR) IV.6 $U_n^2 = U_{n-1} U_{n+1} - (-1)^n$
$V_n^2 = 4(2U_n^2 + (-1)^n) \quad \text{or} \quad V_n^2 - 8U_n^2 = (-1)^n 4$

(PR) IV.7 $U_mV_n - U_nV_m = 2(-1)^nU_{m-n}$

$U_mV_n + U_nV_m = 2U_{m+n}$

(PR) IV.8 $U_n = \sum_{i=0}^{\lfloor (n-1)/2 \rfloor} \binom{n}{2i+1} 2^i$

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

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

(PR) IV.9

m odd $2^{3(m-1)/2}U_k^m = \sum_{i=0}^{(m-1)/2} \binom{m}{i} (-1)^{ki} U_{k(m-2i)}$

$V_k^m = \sum_{i=0}^{(m-1)/2} \binom{m}{i} (-1)^{ki} V_{k(m-2i)}$

m even $2^{3m/2}U_k^m = \sum_{i=0}^{m/2} \binom{m}{i} (-1)^{(k+1)i} V_{k(m-2i)} - \binom{m}{m/2} (-1)^{(k+1)m/2}$

$V_k^m = \sum_{i=0}^{m/2} \binom{m}{i} (-1)^{ki} V_{k(m-2i)} - \binom{m}{m/2} (-1)^{km/2}$

(PR) IV.10

m odd $U_m = \sum_{i=1}^{(m+1)/2} (-1)^{i+1} V_{m+1-2i} + (-1)^{(m+1)/2}$

$U_m = V_{m-1} - V_{m-3} + ... \pm V_0 \mp 1$

$U_m = 2\sum_{i=1}^{\lfloor (m+1)/4 \rfloor} V_{m+2-4i} + 1$

$U_m = 2(V_{m-2} + V_{m-6} + V_{m-10} + ...) + 1$

m even $U_m = \sum_{i=1}^{m/2} (-1)^{i+1} V_{m+1-2i}$

$U_m = V_{m-1} - V_{m-3} + ... \pm V_3 \mp V_1$

$m \equiv 0 \pmod 4$ $U_m = 2\sum_{i=1}^{m/4} V_{m+2-4i}$

$U_m = 2(V_{m-2} + V_{m-6} + V_{m-10} + ... + V_2)$

$m \equiv 2 \pmod 4$ $U_m = 2(\sum_{i=1}^{(m-2)/4} V_{m+2-4i} + 1)$

$U_m = 2(V_{m-2} + V_{m-6} + V_{m-10} + ... + V_4 + 1)$

m odd $2^m = \sum_{i=0}^{(m-2)/2} \binom{m}{i} (-1)^i V_{m-2i} + \binom{m}{m/2} (-1)^{(m)/2}$

$2^m = V_m - \binom{m}{1} V_{m-2} + \binom{m}{2} V_{m-4} - ... \pm 2\binom{m}{(m-1)/2}$

m even $2^m = \sum_{i=0}^{(m-1)/2} \binom{m}{i} (-1)^i V_{m-2i}$

$2^m = V_m - \binom{m}{1} V_{m-2} + \binom{m}{2} V_{m-4} - ... \pm \binom{m}{m/2}$

(PR) IV.11 ...

$({}^{\mathrm{D}}\!/_{\mathrm{p}})$ $({}^{\mathrm{D}}\!/_{\mathrm{p}}) = +1$ when $p \equiv \pm 1 \pmod 8$

$({}^{\mathrm{D}}\!/_{\mathrm{p}}) = -1$ when $p \equiv \pm 3 \pmod 8$

(PR) IV.13 $U_{kp} \equiv 2^{3(p-1)/2} U_k \pmod p$

$U_{p^e} \equiv 2^{3(p-1)e/2} \pmod p$

$U_p \equiv ({}^{\mathrm{D}}\!/_{\mathrm{p}}) \pmod p$

(PR) IV.14 $V_p \equiv 2 \pmod p$

(PR) IV.15 $n, k \geq 1 \quad U_n \mid U_{kn}$

(PR) IV.16 $n, k \geq 1, k$ odd $\quad V_n \mid V_{kn}$

$\rho(p)$ $n \geq 2$, if exists $r \geq 1$ such that $n \mid U_r,$ then$\rho(n)$ is the smallest such r.

(PR) IV.18 $U_n \equiv n \pmod 2$

$V_n \equiv 0 \pmod 2$

$\psi(p)$ $\psi(p) = p - ({}^{8}\!/_{\mathrm{p}})$

(PR) IV.19

$p \equiv \pm 1 \pmod 8$ $\quad p \mid U_{\psi(p)} = U_{p-1}$

$\rho(p) \mid \psi(p) = p - 1$

$p \equiv \pm 3 \pmod 8$ $\quad p \mid U_{\psi(p)} = U_{p+1}$

$\rho(p) \mid \psi(p) = p + 1$

(PR) IV.20 $e \geq 1$ such that $p^e \mid U_m$ and $p^{e+1} \nmid U_m$

if $p \nmid k$ and $f \geq 1$ then $p^{e+f} \mid U_{mkp^f}$

(PR) IV.21 $n \mid U_{\lambda_{\alpha,\beta(n)}}$

$n \mid U_{\psi_{\alpha,\beta(n)}}$

(PR) IV.22

$p \equiv \pm 1 \pmod 8$ $\quad V_{p-1}/2 \equiv +1 \pmod p$

$p \equiv \pm 3 \pmod 8$ $\quad V_{p+1}/2 \equiv -1 \pmod p$

(PR) IV.23

$p \equiv +1 \pmod 8$ $\quad p \mid U_{(p-1)/2}$

$p \equiv +3 \pmod 8$ $\quad p \mid V_{(p+1)/2}$

$p \equiv -3 \pmod 8$ $\quad p \mid U_{(p+1)/2}$

$p \equiv -1 \pmod 8$ $\quad p \mid V_{(p-1)/2}$

(PR) IV.24 $gcd(U_n, V_n) = 1$ or 2

(PR) IV.30

$p \equiv \pm 1 \pmod 8$ $U_{n+p-1} \equiv U_n \pmod p$

$V_{n+p-1} \equiv V_n \pmod p$

The period is: $p-1$.

$p \equiv \pm 3 \pmod 8$ e order of $-1 \pmod p$????

$U_{n+e(p+1)} \equiv U_n \pmod p$

$V_{n+e(p+1)} \equiv V_n \pmod p$

The period is: $e(p+1)$.

1.2 Édouard Lucas and Primality Testing

(HCW) 4.2.12

m-n even $U_m^2 - U_n^2 = U_{m+n}U_{m-n}$

$V_m^2 - V_n^2 = 8U_{m+n}U_{m-n}$

m-n odd $U_m^2 + U_n^2 = U_{m+n}U_{m-n}$

$V_m^2 - V_n^2 = 8U_{m+n}U_{m-n}$

(HCW) 4.3.2 $p^\lambda \neq 2$, if $p^\lambda \parallel U_n$, then $p^{\lambda+1} \parallel U_{pn}$.

(HCW) 4.2.3 $2U_{m+n} = U_mV_n + V_mU_n$

$2V_{m+n} = V_mV_n + 8U_mU_n$

(HCW) 4.2.5 $V_n^2 - 8U_n^2 = 4(-1)^n$

(HCW) 4.2.9 $U_{m+n} = V_mU_n + (-1)^nU_{m-n}$

$V_{m+n} = 8U_mU_n + (-1)^nV_{m-n}$

(HCW) 4.2.13 $V_m^2 - (-1)^{m-n}V_n^2 = 8(U_m^2 - (-1)^{m-n}U_n^2)$

(HCW) 4.2.23 $16U_{2n} = V_{n+1}^2 - V_{n-1}^2$

$2U_{2n} = U_{n+1}^2 - U_{n-1}^2$

1.3 Other properties

MathWorld The Pell Equation: $x^2 - 2y^2 = 1$ is linked with the continued fraction: $\sqrt{2} = [\ 1, \overline{2}\ ]$.
With: $n \geq 1, P_n = Q_n = 1, a_n = 2$, the solutions (p_n, q_n) of: $p_n^2 - 2q_n^2 = 1$ are: n odd, $p_n = (V_{n+1})/2, q_n = U_{n+1}$.

() $V_n(V_m(P,Q), Q^m) = V_{nm}(P,Q)$

(R. Ram) $U_n = 2\sum_{i=1}^{\lfloor \frac{n+1}{2} \rfloor} \binom{n-i}{i-1} 2^{n-2i}$

(R. Melham) $U_n^2 + U_{n-1}U_{n+1} = V_n^2/4$

$V_n^2 + V_{n-1}V_{n+1} = 16U_n^2$

Binomials 1 $0 < k < p$ $\binom{p}{k} \equiv 0 \pmod{p}$

$0 \leq k < p$ $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$

1.4 New (?) properties

(TR) ? $2U_n = \sum_{i=1}^{n-1} V_i$

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

(TR) 1 $V_n + V_{n+1} = 4U_{n+1}$

$V_{n+1} - V_n = 4U_n$

Proof: Use (PR) IV.5b and IV.1 . Same as (PR) IV.5

(TR) 2 $V_n^2 + V_{n+1}^2 = 8U_{2n+1}$

Proof: Use (PR) IV.2 and IV.5a .

(TR) 3 $U_n^2 + U_{n+1}^2 = U_{2n+1}$

Proof: Use (PR) IV.6a and IV.4a .

(TR) 4 $\dfrac{V_n^2 + V_{n+1}^2}{U_n^2 + U_{n+1}^2} = 8$

Proof: Use (TR) 2 and 3 .

(TR) 5 $V_{m+n} + V_{m-n} = 8U_mU_n$ (n odd) (for $m \geq n$)

$V_{m+n} + V_{m-n} = V_mV_n$ (n even) (for $m \geq n$)

Proof: Use (PR) IV.4b and IV.3b .

(TR) 6 $U_{m+n} + U_{m-n} = V_m U_n$ (n odd) (for $m \geq n$)

$U_{m+n} + U_{m-n} = U_m V_n$ (n even) (for $m \geq n$)

Proof: Use (PR) IV.7 and IV.3a .

(TR) 7 $U_{m+n}^2 - U_{m-n}^2 = U_{2m} U_{2n}$ (for $m \geq n$)

Proof: Use (PR) IV.3 and IV.7 .

(TR) 8 $\dfrac{V_{m+n}^2 - V_{m-n}^2}{U_{m+n}^2 - U_{m-n}^2} = 8$ (for $m \geq n$)

or: $\dfrac{V_m^2 - V_n^2}{U_m^2 - U_n^2} = 8$ (for $m - n$ even ≥ 0)

Proof: Use (PR) IV.6b and (TR) 7 .

(TR) 9 $V_{m+n}^2 - V_{m-n}^2 = 8 U_{2m} U_{2n}$ (for $m \geq n$)

Proof: Use (TR) 7 and 8 .

(TR) 9 bis $\dfrac{V_m^2 + V_n^2}{U_m^2 + U_n^2} = 8$ (for $m - n$ odd)

Proof: Use (PR) IV.6b .

$V_m^2 + V_n^2 = 8 U_{m+n} U_{m-n}$ (for $m - n$ odd ≥ 0)

Proof: ???? .

$U_m^2 + U_n^2 = U_{m+n} U_{m-n}$ (for $m - n$ odd ≥ 0)

Proof: ???? .

(TR) 10 $U_{2^n} = \prod_{i=0}^{n-1} V_{2^i}$ (for $n \geq 1$)

Proof: Use (PR) IV.2a .

(TR) 11 $V_{2n} = 2(4U_n^2 + (-1)^n)$ (for $n \geq 1$)

Proof: Use (PR) IV.3b and IV.6b .

(TR) 12 $V_{2^n} = 2(4U_{2^{n-1}}^2 + 1)$ (for $n \geq 2$)

Proof: Use (TR) 11 .

(TR) 13a $V_{2^n} = 2(4(\prod_{i=0}^{n-2} V_{2^i})^2 + 1)$ (for $n \geq 2$)

and: $V_{2^n} \equiv 2 \pmod{2^{2n+1}}$ (for $n \geq 2$)

And thus, the factors f_i of $V_{2^n}/2$ are of the form: $f_i \equiv 1 \pmod{2^{n+2}}$

Proof: Use (TR) 11 and 12 .

(TR) 13b n even

$$U_{2n+1} = U_{n+1}V_n - 1$$
$$U_{2n-1} = U_nV_{n-1} + 1$$
$$V_{2n+1} = V_{n+1}V_n - 2$$
$$V_{2n-1} = V_nV_{n-1} + 2$$

Proof: (PR) IV.3 .

(TR) 13b n odd

$$U_{2n+1} = U_{n+1}V_n + 1$$
$$U_{2n-1} = U_nV_{n-1} - 1$$
$$V_{2n+1} = V_{n+1}V_n + 2$$
$$V_{2n-1} = V_nV_{n-1} - 2$$

Proof: (PR) IV.3 .

(TR) 13c $\frac{V_{2^n-1}}{2} \equiv -1 \pmod{2^{n+1}}$ (for $n \geq 2$)

$\frac{V_{2^n+1}}{2} \equiv +1 \pmod{2^{n+1}}$ (for $n \geq 2$)

Proof:
This is true for n=2 : $V_{2^2-1} = 2(2^3 * 1 - 1), V_{2^2+1} = 2(1 + 2^3 * 5)$
Thus by (TR) 13b:
$V_{2^{n+1}-1} = V_{2^n}V_{2^n-1} + 2 = 2\big[2(1 + 2^{2n}k_0^2)(2^{n+1}k_{-1} - 1) + 1\big]$
and: $V_{2^{n+1}-1} = 2(2^{n+2}k'_{-1} - 1)$
$V_{2^{n+1}+1} = V_{2^n}V_{2^n+1} - 2 = 2\big[2(1 + 2^{2n}k_0^2)(1 + 2^{n+1}k_{+1}) - 1\big]$
and: $V_{2^{n+1}+1} = 2(1 + 2^{n+2}k'_{+1})$

(TR) N1 $V_n = 2\big(2\sum_{i=0}^{n-1} U_i + 1\big)$

Proof: (PR) IV.1 and (PR) IV.5f .

(TR) N2 $2U_n = \sum_{i=0}^{n-1} V_i$

Proof: ????

(TR) N3 $2U_n^2 = \sum_{i=0}^{2n-1} U_i \quad n$ even

Proof: ????

$V_n^2 = 4\sum_{i=0}^{2n-1} U_i \quad n$ odd

$4\sum_{i=0}^{n-1} U_i = V_n - V_0$

Proof: ????

(TR) N4 $2\sum_{i=0}^{2n} U_i = \sum_{i=1}^{n} V_{2i}$

Proof: ????

$2\sum_{i=0}^{2n+1} U_i = \sum_{i=0}^{n} V_{2i+1}$

Proof: ????

(TR) N5 $4\sum_{i=0}^{2n} U_i + 2U_{2n+1} = \sum_{i=1}^{2n+1} V_i$

Proof: ????

$U_{2n} - U_{2n-1} = 2\sum_{i=0}^{2(n-1)} U_i + 1$

Proof: ????

$\sum_{i=0}^{n} U_i = \frac{1}{2}(U_{n+1} + U_n - 1)$

Proof: ????

(TR) 14 $V_{n+1} - V_{n-1} = 2V_n$
Proof: Use (PR) IV.3b .

(TR) 15 $U_{n+2} - U_{n-2} = V_{n+1} - V_{n-1} = 2V_n$
Proof: Use (PR) IV.10 and (TR) 14 .

(TR) 16 $U_{n+1} + U_{n-1} = V_n$
Proof: Use (PR) IV.10 or IV.3a . (Same as (PR) IV.5)

(TR) 17 $2\sum_{i=0}^{n} U_i^2 = U_n U_{n+1}$
Proof: ??

(TR) 18 $2\sum_{i=0}^{n} V_i^2 = V_{2n+1} + 4 + 2(-1)^n$

$2\sum_{i=0}^{n} V_i^2 = V_n V_{n+1} + 4$
Proof: ??

(TR) 19 $2\sum_{i=0}^{n} U_i = U_n + U_{n+1} - 1$
Proof: ??

(TR) 20 $2\sum_{i=0}^{n} V_i = V_n + V_{n+1}$

or $2\sum_{i=0}^{n-2} V_i = V_{n+1} - V_n$

Proof: ??

(TR) 21 $2\sum_{i=0}^{n} iU_i = nU_n + (n-1)U_{n+1} + 1$

$2\sum_{i=0}^{n} iV_i = nV_n + (n - 1V_{n+1} + 2$

Proof: ??

(TR) 22 $U_n = 2^{n-1} + \sum_{i=1}^{n-2} 2^{i-1} U_{n-1-i}$

$V_n = 2^n + \sum_{i=1}^{n-1} 2^{i-1} V_{n-1-i}\ ,\quad n \geq 1$

or $V_n = 2^n + 2^{n-1} + \sum_{i=1}^{n-2} 2^{i-1} V_{n-1-i}\ ,\quad n \geq 2$

or $V_n = 2^n + 2^{n-1} + 2^{n-2} + \sum_{i=1}^{n-3} 2^{i-1} V_{n-1-i}\ ,\quad n \geq 3$

Proof: A. T. Benjamin and Jennifer J. Quinn for U_n property:
"The Fibonacci Numbers - Exposed More Discretely"

(TR) 23 $\sum_{i=0}^{2n} \binom{2n}{i} U_{2i} = 8^n U_{2n}$

$\sum_{i=0}^{2n} \binom{2n}{i} V_{2i} = 8^n V_{2n}$

Proof:

(TR) 24 $V_{2m} \equiv 2(2^{m+1} - 1) \pmod{(2m+1)}$ When $2m + 1$ is prime.

Proof: $V_{2m} = 2\sum_{i=0}^{m} \binom{2m}{2i} 2^i \equiv 2\sum_{i=0}^{m} 2^i \pmod{(2m+1)}$

$0 \leq 2i < 2m\ :\quad \binom{2m}{2i} \equiv (-1)^{2i} = 1 \pmod{(2m+1)}$

See (Binomials 1)

For: $m = 2^{2^n - 1},\ F_n$ prime $\Rightarrow 2^{2^{2^n-1}+1} \equiv 1 \pmod{F_n}$.

(TR) 25 $\sum_{i=0}^{n} \frac{1}{V_{2^i}} = \frac{\sum_{i=0}^{n} U_{2^i} \prod_{j=i+1}^{n} V_{2^j}}{U_{2^{n+1}}}$

$\sum_{i=0}^{n} \frac{1}{U_{2^i}} = \frac{1 + \sum_{i=0}^{n} \prod_{j=i}^{n} V_{2^j}}{U_{2^n}}$

Proof:

(TR) 26 $1+\sum_{i=0}^{n}\prod_{j=i}^{n}V_{2^j}=U_{2^{n+1}-1}+V_{2^{n+1}-1}$

$\sigma_n=1+\sum_{i=0}^{n}2i=n^2+n+1$

$1+\sum_{i=0}^{n}\prod_{j=i}^{n}V_{2j}=U_{\sigma_n}+V_{\sigma_n}+X_n$

$X_1=X_2=0\ ,\ X_3=4*1\ ,\ X_4=4*1182\ ,\ X_5=4*7955627...$

Proof:

(TR) 27 $V_n\big(U_{n+m}+V_{n+m}\big)-\big(U_m+V_m\big)Q^n=U_{2n+m}+V_{2n+m}$

$n\in Z\ ,\ m\in Z$

$V_{2^n}\big(U_{2^n+m}+V_{2^n+m}\big)-\big(U_m+V_m\big)(-1)^n=U_{2^{n+1}+m}+V_{2^{n+1}+m}$

$n\in N\ ,\ m\in Z$

Proof: (PR) IV.3

(TR) 28 $V_{2^n}\big(U_{2^n-1}+V_{2^n-1}\big)+1=U_{2^{n+1}-1}+V_{2^{n+1}-1}$

$U_{2^n}\big(8U_{2^n-1}+V_{2^n-1}\big)-1=U_{2^{n+1}-1}+V_{2^{n+1}-1}$

$U_{2^n-1}\big(8U_{2^n}-V_{2^n}\big)+V_{2^n-1}\big(U_{2^n}-V_{2^n}\big)=2$

Proof:

(TR) 29 $W_n=-(U_n+V_n)\ ,\ n\in Z$

???? $W_m+\sum_{i=0}^{1}\prod_{j=i}^{n}V_{2^i}+\sum_{i=2}^{n}W_m\prod_{j=i}^{n}V_{2^i}=U_{2^{n+1}-m}+V_{2^{n+1}-m}$

Proof: C'est faux !!

(TR) 30 ${V_n}^2-8{U_{n-1}}^2=2V_{2n-1}$

Proof: ??

(TR) 31 $V'_0=1,V'_n=V_n\ ,n\geq 1$

Let: $A_n=2\sum_{i=0}^{\lfloor (n-2)/4\rfloor}V'_{4i+(n \bmod 4)+2}$

$U_n=A_n\ ,\ n$ even.

$U_n=A_n+1\ ,\ n$ odd.

Proof: ??

(TR) 32 $8U_2 \sum_{i=0}^{n-1} U_{4i+0} = V_{4n-2} - V_{-2}$

$8U_2 \sum_{i=0}^{n-1} U_{4i+1} = V_{4n-1} - V_{-1}$

$8U_2 \sum_{i=0}^{n-1} U_{4i+2} = V_{4n+0} - V_0$

$8U_2 \sum_{i=0}^{n-1} U_{4i+3} = V_{4n+1} - V_1$

Proof: ??

(TR) 32' $V_{4n+b} - V_b = 8U_2 \sum_{i=0}^{n-1} U_{4i+b+2} \quad b = -2 \dots 1$

Proof: ??

(TR) 33 $V_{8n+b} - V_b = 8U_4 \sum_{i=0}^{n-1} U_{8i+b+4} \quad b = -4 \dots 3$

Proof: ??

(TR) 34 $V_{2^k n+b} - V_b = 8U_{2^{k-1}} \sum_{i=0}^{n-1} U_{2^k i+b+2^{k-1}} \quad b = -2^{k-1} \dots 2^{k-1} - 1$

Proof: ??

(TR) 35 $V_{2n+1}^2 = 2 \sum_{i=0}^{2n} V_{2i+1}$

$U_{2n}^2 = \sum_{i=0}^{2n-1} (-1)^{i+1} U_{2i+1}$

$V_{2n} = 2 \sum_{i=0}^{n-1} V_{2i+1} + 2$

$U_{2n} = 2 \sum_{i=0}^{n-1} U_{2i+1}$

$V_{2n+1} = 2 \sum_{i=0}^{n} V_{2i} - 2$

$U_{2n+1} = 2 \sum_{i=0}^{n} U_{2i} + 1$

Proof: ??

2 Pell numbers modulo a Fermat number

We describe hereafter the properties of the Pell numbers modulo the Fermat numbers F_2, F_3, F_4 (primes) and F_5 (composite).

2.1 Pell numbers $\pmod{F_2}$

There is a period of $16 = F_2 - 1$ amongst the values of U_i and $V_i \pmod{F_2}$. We also have the following symmetries:

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

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

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 2: F_2

Examples:

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

Noticeable values: $U_2 \equiv 2^1$, $V_2 \equiv 2^3 - 2^1$, $U_{2^2} \equiv 2^3 + 2^2 \pmod{F_2}$.

2.2 Pell numbers (mod F_3)

Now, the period is: $128 = \frac{F_3-1}{2}$.
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:

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

Noticeable values: $U_{16} \equiv 2^3$, $V_{16} \equiv -(2^6 - 2^2)$, $V_{31} \equiv 2^3F_2$, $U_{2^5} \equiv 2^5 + 2^1 \equiv 2^1F_2 \pmod{F_3}$.

2.3 Pell numbers (mod F_4)

Now, the period is: $8192 = \frac{F_4-1}{8}$.
We find for F_4 the same kind of symmetries we had for F_2 and 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 3: F_3

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 4: F_4

Noticeable values: $U_{1024} \equiv -2^7$, $V_{1024} \equiv 2^{12} - 2^4$, $U_{2046} \equiv 24F_3$, $V_{2046} \equiv -2^6 F_3$, $U_{2047} \equiv -2^3 F_3$, $V_{2047} \equiv 2^5 F_3$, $U_{2^{1}1} \equiv 2^{11} + 2^3 \equiv 2^3 F_3 \pmod{F_4}$.

2.4 Pell numbers $\pmod{F_5}$

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 5: F_5

Here, the period is: $11167360 = 2^7 \times 5 \times 17449$.
Since: $F_5 = f_1 \times f_2$ and $f_1 = 641 = 1+5\times2^7$, $f_2 = 6700417 = 1+3\times17449\times2^7$, it appears that the period is equal to: $((f_1-1)(f_2-1))/(3\times2^7)$.

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

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

2.5 Properties linked with ...

(TR) 14 Relationships with Fermat numbers.

$V_{2^2} \equiv 0 \pmod{F_2}$
and $V_{2^1} \equiv 6 = 2^{3\times 1} - 2^1 = 2F_0 = (F_0 - 1)(F_1 - 2) \pmod{F_2}$
and $6^2 - 2 = 2(2^1 - 1)F_2$

$V_{2^5} \equiv 0 \pmod{F_3}$
and $V_{2^4} \equiv 60 = 2^{3\times 2} - 2^2 = 4F_0F_1 = (F_1 - 1)(F_2 - 2) \pmod{F_3}$
and $60^2 - 2 = 2(2^3 - 1)F_3$

$V_{2^{11}} \equiv 0 \pmod{F_4}$
and $V_{2^{10}} \equiv 4080 = 2^{3\times 4} - 2^4 = 16F_0F_1F_2 = (F_2 - 1)(F_3 - 2) \pmod{F_4}$
and $4080^2 - 2 = 2(2^7 - 1)F_4$

$V_{2^{3\times 2^{n-2}-1}} \equiv 0 \pmod{F_n}$ iff F_n is prime ??

Let: $\alpha_n = 2^{3\times 2^{n-2}} - 2^{2^{n-2}} = 2^{2^{n-2}} \prod_{i=0}^{n-2} F_i = (F_{n-2} - 1)(F_{n-1} - 2)$

$(\alpha_n)^2 - 2 = 2(2^{2^{n-1}-1} - 1)F_n \quad$ (for $n \geq 2$)

Il faut montrer:
F_n prime $\Longrightarrow F_n \mid V_{etc}$

(PRIV.3 $U_{m+n} = U_{m-n} \pmod{F_n}$ n odd
$U_{m+n} = -U_{m-n} \pmod{F_n}$ n even

Let: $\begin{cases} \mathfrak{F} = F_n - 1 \\ \mathfrak{F}_1 = (F_n - 1)/2^1 = 2^{2^{n-1}} \\ \mathfrak{F}_2 = (F_n - 1)/2^2 \\ \mathfrak{F}_m = (F_n - 1)/2^m \end{cases}$

(TR) X1 $U_1 + U_3 + ... + U_{\mathfrak{F}_m - 1} = \sum_{i=0}^{\mathfrak{F}_{m-1}-1} U_{2i+1} \equiv 0 \pmod{F_n}$
$m = 1$ or 2.

Proof:

If $\mathfrak{F}$ is prime then: $U_{\mathfrak{F}} \equiv 0 \pmod{F_n}$.

By (TR) N3a, we have:
$\sum_{i=0}^{2^{2^n+1}-1} U_i = U_0 + U_{\mathfrak{F}} + \sum_{i=1}^{\mathfrak{F}-1}(U_i + U_{\mathfrak{F}+i}) = 2U_{\mathfrak{F}}^2 \equiv 0 \pmod{F_n}$

Since: $U_0 + U_{\mathfrak{F}} \equiv 0 \pmod{F_n}$ then:

$\sum_{i=1}^{\mathfrak{F}-1}(U_i + U_{\mathfrak{F}+i}) = \sum_{i=1}^{\mathfrak{F}_1-1}(U_{\mathfrak{F}+2i} + U_{\mathfrak{F}-2i}) + \sum_{i=0}^{\mathfrak{F}_1-1}(U_{\mathfrak{F}+(2i+1)} + U_{\mathfrak{F}-(2i+1)})$

By (PR) IV.3 n even: $\sum_{i=1}^{\mathfrak{F}_1-1}(U_{\mathfrak{F}+2i} + U_{\mathfrak{F}-2i}) \equiv 0 \pmod{F_n}$ and:

$\sum_{i=0}^{\mathfrak{F}_1-1}(U_{\mathfrak{F}+(2i+1)} + U_{\mathfrak{F}-(2i+1)}) = 2\sum_{i=0}^{\mathfrak{F}_1-1} U_{2i+1}$

Finally: $U_1 + U_3 + ... + U_{\mathfrak{F}-1} = \sum_{i=0}^{\mathfrak{F}_1-1} U_{2i+1} \equiv 0 \pmod{F_n}$ $\square$

$U_{\mathfrak{F}_1} \equiv 0 \pmod{F_n}$

N3a $\Longrightarrow \sum_{i=0}^{2\mathfrak{F}-1} U_i = U_0 + U_{\mathfrak{F}_1} + \sum_{i=1}^{\mathfrak{F}_1-1}(U_i + U_{\mathfrak{F}_1+i}) = 2U_{\mathfrak{F}_1}^2 \equiv 0 \pmod{F_n}$

$U_0 + U_{\mathfrak{F}_1} \equiv 0 \pmod{F_n}$

$\sum_{i=1}^{\mathfrak{F}_1-1}(U_i + U_{\mathfrak{F}_1+i}) = \sum_{i=1}^{\mathfrak{F}_2-1}(U_{\mathfrak{F}_1+2i} + U_{\mathfrak{F}_1-2i}) + \sum_{i=0}^{\mathfrak{F}_2-1}(U_{\mathfrak{F}_1+(2i+1)} + U_{\mathfrak{F}_1-(2i+1)})$

$\sum_{i=1}^{\mathfrak{F}_2-1}(U_{\mathfrak{F}_1+2i} + U_{\mathfrak{F}_1-2i}) \equiv 0 \pmod{F_n}$

$\sum_{i=0}^{\mathfrak{F}_2-1}(U_{\mathfrak{F}_1+(2i+1)} + U_{\mathfrak{F}_1-(2i+1)}) = 2\sum_{i=0}^{\mathfrak{F}_2-1} U_{2i+1}$

Finally: $U_1 + U_3 + ... + U_{\mathfrak{F}_1-1} = \sum_{i=0}^{\mathfrak{F}_2-1} U_{2i+1} \equiv 0 \pmod{F_n}$

3 Properties of the LLT

Let's say: $\mathcal{L}(x) = x^2 - 2$, $\mathcal{L}^1 = \mathcal{L}$, $\mathcal{L}^m = \mathcal{L} \circ \mathcal{L}^{m-1} = \mathcal{L} \circ \mathcal{L} \circ \mathcal{L} \ldots \circ \mathcal{L}$. Where $\mathcal{L}$ is the function used in the Lucas-Lehmer Test (LLT) : $S_0 = 4$, $S_{i+1} = S_i^2 - 2 = \mathcal{L}(S_i)$; M_q is prime $\iff S_{q-2} \equiv 0 (\mathrm{mod}\ M_q)$.
Let's call $\mathcal{C}_m^+$ the sum of the positive coefficients of $\mathcal{L}^n(x)$ and $\mathcal{C}_m^-$ the sum of the negative coefficients of $\mathcal{L}^m(x)$. $\mathcal{C}_1^+ = 1,\ \mathcal{C}_2^+ = 3,\ \mathcal{C}_3^+ = 23,\ \mathcal{C}_4^+ = 1103$.

Numerical experiments show the following properties (where $F_n = 2^{2^n} + 1$ is a prime Fermat number, and $M_q = 2^q - 1$ is a prime Mersenne number):

$$\mathcal{C}_m^+ \text{ is odd, and } \mathcal{C}_m^+ + \mathcal{C}_m^- = -1 \text{ , for: } m \geq 1 \quad \text{LLT.1}$$

$$\mathcal{C}_m^+ = 2^m \prod_{i=1}^{m-1} \mathcal{C}_i^+ - 1 \quad \text{for: } m > 1 \quad \text{LLT.2}$$

$$\mathcal{C}_m^+ \equiv 3 \pmod{5} \quad \text{for: } m \geq 1 \quad \text{LLT.3}$$

$$p \text{ prime, } p \mid \mathcal{C}_m^+ \iff p = 2^m 3k - 1 (k \text{ odd}), \text{ or } p = 2^{m+1} 3k' + 1 \quad \text{LLT.4}$$

$$\text{The period of } \mathcal{C}_m^+ \pmod{F_n} \text{ is: } 2^n - 1 \quad n \geq 1 \quad \text{LLT.5}$$

$$\prod_{i=1}^{2^n-1} \mathcal{C}_i^+ \equiv 1 \pmod{F_n} \quad \text{LLT.6}$$

$$\mathcal{C}_{m \equiv 1 \pmod{2^n-1}}^+ \equiv -2 \pmod{F_n} \quad \text{for: } m > 1 \quad \text{LLT.7}$$

$$\text{The period of } \mathcal{C}_m^+ \pmod{M_q} \text{ is: } q-1 \quad \text{for: } q \equiv 1 \pmod 4 \quad \text{LLT.8}$$

$$\mathcal{C}_m^+ \equiv 2^{q-1} \pmod{M_q} \quad \text{for: } m > q \quad \text{and: } \quad q \equiv -1 \pmod 4 \quad \text{LLT.9}$$

$$\mathcal{C}_m^+ \equiv 2^q - 1 \pmod{2^q} \quad \text{for: } m \geq q \quad \text{LLT.10}$$

Properties LLT.5, LLT.6 and LLT.7 could be used as a primality test for Fermat numbers, and properties LLT.8 and LLT.9 could be used as a primality test for Mersenne numbers, once proven ... But they would not lead to a faster test than Pépin's or LLT tests.

Examples:
$\mathcal{L}^2(x) = x^4 - 4x^2 + 2$
$\mathcal{L}^3(x) = x^8 - 8x^6 + 20x^4 - 16x^2 + 2$
$\mathcal{L}^4(x) = x^{16} - 16x^{14} + 104x^{12} - 352x^{10} + 660x^8 - 672x^6 + 336x^4 - 64x^2 + 2$

$\mathcal{C}_2^+ = 4 \times 1 - 1 = 3$,
$\mathcal{C}_3^+ = 8 \times 1 \times 3 - 1 = 23$,
$\mathcal{C}_4^+ = 16 \times 1 \times 3 \times 23 - 1 = 1103$,
$\mathcal{C}_5^+ = 32 \times 1 \times 3 \times 23 \times 1103 - 1 = 2435423$

$n > 1$

$\bullet F_1 = 5$
$n > 2 : \mathcal{C}_n^+ \equiv 3 = (F1 - 2 + F_0)/2 \equiv -2 \pmod{F_1}$

$\bullet F_2 = 17$
$n = 0 \pmod{2^2 - 1} : \mathcal{C}_n^+ \equiv 6 = (F_2 - 2 + F_1)/2 - 4 \pmod{F_2}$
$n = 1 \pmod{2^2 - 1} : \mathcal{C}_n^+ \equiv -2 \pmod{F_2}$
$n = 2 \pmod{2^2 - 1} : \mathcal{C}_n^+ \equiv 3 \pmod{F_2}$

$\bullet F_3 = 257$
$n = 0 \pmod{2^3 - 1} : \mathcal{C}_n^+ \equiv 136 = (F_3 - 2 + F2)/2 \pmod{F_3}$
$n = 1 \pmod{2^3 - 1} : \mathcal{C}_n^+ \equiv -2 \pmod{F_3}$
$n = 2 \pmod{2^3 - 1} : \mathcal{C}_n^+ \equiv 3 \pmod{F_3}$
$n = 3 \pmod{2^3 - 1} : \mathcal{C}_n^+ \equiv 23 \pmod{F_3}$
$n = 4 \pmod{2^3 - 1} : \mathcal{C}_n^+ \equiv 75 \pmod{F_3}$
$n = 5 \pmod{2^3 - 1} : \mathcal{C}_n^+ \equiv 91 \pmod{F_3}$
$n = 6 \pmod{2^3 - 1} : \mathcal{C}_n^+ \equiv 38 \pmod{F_3}$

$\bullet F_4 = 65537$
$n = 0 \pmod{2^4 - 1} : \mathcal{C}_n^+ \equiv 32896 = (F_4 - 2 + F_3)/2 \pmod{F_4}$
$n = 1 \pmod{2^4 - 1} : \mathcal{C}_n^+ \equiv -2 \pmod{F_4}$
$n = 2 \pmod{2^4 - 1} : \mathcal{C}_n^+ \equiv 3 \pmod{F_4}$
...

$n = 15 \pmod{2^4 - 1} : \mathcal{C}_n^+ \equiv 23133 \pmod{F_4}$

$\bullet F_2 :\quad 3 \times 6 \equiv 1 \pmod{F_2}$
$\bullet F_3 :\quad 3 \times 23 \times 75 \times 91 \times 38 \times 136 \equiv 1 \pmod{F_3}$
$\bullet F_4 :\quad 3 \times 23 \times 1103 \times \ldots \times 32896 \equiv 1 \pmod{F_4}$

4 NSW numbers

$W_0 = S_1 = 1,\ W_1 = S_3 = 7,\ W_2 = S_5 = 41,\ W_3 = S_7 = 239$

n	0	1	2	3	4	5	6	7	8
W_n	1	7	41	239	1393	8119	47321	275807	1607521

Table 6: First NSW numbers

$$W_n(6,1) = S_{2n+1} = \frac{V_{2n+1}(2,-1)}{2} \quad , W_0 = 1\ , W_1 = 7$$

S_{2n+1} prime $\implies$ $2n+1$ prime
S_p is prime for: $3, 5, 7, 19, 29, 47, 59, 163, 257, 421, 937, 947, 1493, 1901, 6689, 8087, 9679.$
S_p is PRP-prime for: $28953, 79043.$

$$W_{2n} = W_n^2 - \sum_{i=0}^{2n-1} W_i$$

$$W_{2n+1} = W_n W_{n+1} - \sum_{i=1}^{2n-1} W_i$$

$$W_n^2 + W_{n+1}^2 = 6 W_n W_{n+1} + 8$$

$$W_{n+1}^2 - W_{n-1}^2 = W_n (W_{n+2} - W_{n-2})$$

$$W_n^2 = \frac{V_{2(2n+1)}(2,-1) - 2}{4}$$