Quadrature nº 42 (2024) 1-8

The Wagstaff numbers (v3)

Everything You Always Wanted to Know About Them (But Were Afraid to Ask)

par Tony REIX*

Résumé.

After a description of the Wagstaff numbers, the paper recalls the known methods used for finding Wagstaff PRPs (PRobably Prime) and it provides the current world record. Then it describes the characteristics of the DiGraphs (Directed Graph) generated by x^2-2 for the Mersenne, Fermat and Wagstaff numbers. It provides the weird link between the number of Cycles of length $q-1$ and $q-2$ of the DiGraph under x^2-2 modulo a Wagstaff prime and the OEIS series A165921 defined from irreducible polynomials. Then, it shows that a Primality Test for Fermat numbers built by means of the Elliptic Curve theory seems to work also for the Wagstaff numbers, and - again - it shows a surprising link between the number of Cycles of length $q-2$ of the DiGraph under $\frac{x^4+2x^2+1}{4(x^3-x)}$ modulo a Wagstaff prime and the OEIS series A165921. Last, it provides the graphic display of several DiGraphs under $\frac{x^4+2x^2+1}{4(x^3-x)}$ modulo Fermat and Wagstaff primes, with details, showing the main BigTrees and main Cycles.

The goal of this paper is to create interest for the Wagstaff numbers and for the search for an efficient method for proving that a Wagstaff PRP is a true prime.

I Introduction

The Wagstaff numbers are cousins of the Fermat numbers and german cousins of the Mersenne numbers. However, they are not smooth as the others are... and thus no fast Primality Test is known for them. We only know fast PRP tests for them, often based on the Lucas-Lehmer Test technic. Here after is described a new potential method, based on a recent Primality Test for Fermat numbers built on Elliptic Curves.

II Wagstaff numbers

II.1 Definition and status

A Wagstaff number is : $W_q = \frac{2^q+1}{3}$.

If W_q is prime, thus q is prime.

It is a RepUnit $R_n^{(b)} = \frac{b^n-1}{b-1}$ with base $b=-2$.

We have : $W_q = 1+2\sum_{i=0}^{\frac{q-3}{2}} 4^i = 1+2qk$.

And, with $M_k = 2^k-1$: $W_q = 1+2M_{\frac{q-1}{2}}W_{\frac{q-1}{2}}$. Thus q prime divides either $M_{\frac{q-1}{2}}$ or $W_{\frac{q-1}{2}}$.

Thus, a Wagstaff number is not *smooth* (it does not write as : $W_q = N+1$ or $N-1$ where N is completely or partially factorized).

There are 34 known Wagstaff primes and 10 Wagstaff PRPs (PRobably Prime). Values of q for first Wagstaff primes are : $3,5,7,11,13,17,19,23,31,\ldots$ First non-prime Wagstaff number appears with $q=29$. See sequence A000978 in the OEIS project.

* tony.reix@laposte.net

For now, a Wagstaff PRP can be proved prime by using a distributed ECPP implementation, as it was done for $q = 42,737$ (12,865 digits) by François Morain in 2007 after I warned him about this W_q being withing range, or for $q = 127,031$ in January 2023.

In 2010, as part of a team (DUR project : Vincent Diepeveen, Paul Underwood, Tony Reix), I discovered the candidate Wagstaff PRP Record $W_{4,031,399}$, using the Vrba-Reix test implemented in the *LLR* tool by Jean Penné of the GIMPS project. Then, thanks to complementary tests, it was proved to be a full PRP.

Then, three new Wagstaff PRPs have been found : $W_{13,347,311}$, $W_{13,372,531}$ and $W_{15,135,397}$, partly using the work of our DUR project on checking Wagstaff prime exponents.

II.2 Search of Wagstaff PRPs

For more than 20 years, several PRP tests for Wagstaff numbers were found and proven for finding Wagstaff PRPs (plus many conjectures), based on several technics (like the Lucas-Lehmer Sequences, used for the LLT test for Mersenne numbers and used for a LLT-similar test for Fermat numbers). Here are some of them :

Theorem 1 (Lifchitz Renaud & Henri - 2000 July)**.** *$N_p = 2^p + 1$ and $W_p = \frac{N_p}{3}$. If W_p is a prime, then* $25^{2^{p-1}} \equiv 25 \pmod{N_p}$.

Theorem 2 (Vrba Anton & Reix Tony - àla LLT - Group Theory)**.** *Let $S_{n+1} = S_n^2 - 2$ and p be a prime larger than 3. If $W_p = \frac{2^p+1}{3}$ is a prime, then $S_p \equiv S_2 \pmod{W_p}$ where $S_0 = 6$.*

Theorem 3 (Gerbicz Robert - àla LLT)**.** *Let $q > 3$ a prime, and $p = W(q) = \frac{2^q+1}{3}$ is also prime (Wagstaff prime), then for the sequence $S_0 = \frac{3}{2}$, $S_{k+1} = S_k^2 - 2$, it is true that $S_q - S_1$ is divisible by p .*

Theorem 4 (Reix - àla Pépin - Proof based on a Lucas Sequence)**.** *If $W_q = \frac{2^q+1}{3}$ (q prime $\geqslant 7$) is a prime , then : $7^{\frac{W_q-1}{2}} \equiv -1 \pmod{W_q}$.*

Theorem 5 (Reix - Proof based on a Lucas Sequence)**.** *If $W_q = \frac{2^q+1}{3}$ (q prime $\geqslant 7$) is a prime, then : $S_q \equiv S_2 \pmod{W_q}$, with : $S_0 = 8$ and $S_n = (S_{n-1} - 1)^2 + 1$.*

Theorem 6 (Reix - àla LLT - Proof based on a Lehmer Sequence)**.** *If $W_q = \frac{2^q+1}{3}$ (q prime $\geqslant 11$) is a prime, then : $S_q \equiv S_2 = 1154 \pmod{W_q}$, with : $S_0 = 6$ and $S_i = S_{i-1}^2 - 2$ for $i = 1,2,3,... q$.*

Theorem 7 (Paul Underwood - àla LLT)**.** *If $W_q = \frac{2^q+1}{3}$ ($q \equiv \pm 1 \pmod 6$) is a prime, then : $S_{q-2} \equiv \pm 4 \pmod{W_q}$, with : $S_0 = 4$ and $S_i = S_{i-1}^2 - 2$ for $i = 1,2,3,...$ and q prime $\geqslant 7$.*

Conjecture 1 (Reix - àla LLT)**.** *If $W_q = \frac{2^q+1}{3}$ (q prime $\geqslant 7$) is a prime, then : $S_{q-1} \equiv S_0 \pmod{W_q}$, with : $S_0 = 7^2 + 1/7^2$ and $S_i = S_{i-1}^2 - 2$ for $i = 1,2,3,... q-1$.*

III DiGraph under $x^2 - 2$

Vasiga & Shallit ([1] : *On the iteration of certain quadratic maps over GF(p)*) studied the DiGraph under $x^2 - 2$ modulo a Mersenne and a Fermat number, proving that, for both kinds of numbers, their DiGraph is made of one Big Tree and of many Cycles.

III.1 ... modulo a Mersenne number

The LLT test for Mersenne numbers ($2^q - 1$, q prime) makes use of the Big Tree of the DiGraph under $x^2 - 2$ modulo a Mersenne number, starting from one of the 3 universal seeds (4, 10, 2/3) and then reaching 0 after $q - 1$ steps.

Theorem 8 (Lucas-Lehmer Primality Test for Mersenne numbers)**.** *$M_q = 2^q - 1$ (with q prime) is a prime iff $S_{q-1} \equiv 0 \pmod{M_q}$, with : $S_0 = 4$ and $S_i = S_{i-1}^2 - 2$ for $i = 1,2,3,...$.*

I had found and provided the formula generating the number of Cycles of such a DiGraph under $x^2 - 2$:

Theorem 9 (Reix - ZetaX (from *Art of Problem Solving* forum) - 2)**.** *The number of cycles of length L (L divides $q - 1 = 2^s u$) in the digraph $G_{x \to x^2-2}$ modulo a Mersenne prime $2^q - 1$ is :*

$$\varsigma(L) = \frac{1}{L}\left(\sum_{d|L} \mu\left(\frac{L}{d}\right) 2^d - \sum_{2^s|d|L} \mu\left(\frac{L}{d}\right) 2^{d-1}\right)$$

III.2 ... modulo a Fermat number

A LLT-based primality test for Fermat numbers ($F_n = 2^{2^n} + 1$) makes use of the Big Tree of the DiGraph under $x^2 - 2$ modulo a Fermat number, starting from the universal seed 5 and then reaching 0 after $2^n - 2$ steps. There exist 4 proofs of a similar primality test for Fermat numbers, including mine. It is not known if there exist several universal seeds. And the PÃ©pin's test can be proved by means of the Lucas-Lehmer Sequence technic.

Theorem 10 (Lucas-Lehmer-Reix Primality Test for Fermat numbers)**.** *$F_n = 2^{2^n} + 1$ ($n \geq 1$) is a prime iff $S_{2^n-2} \equiv 0 \pmod{F_n}$, with : $S_0 = 5$ and $S_i = S_{i-1}^2 - 2$ for $i = 1,2,3,...$.*

III.3 Use of a Cycle instead of the Big Tree

It is conjectured that it is possible to prove that a Mersenne or a Fermat number is prime by using a Cycle of such a DiGraph under x^2-2 rather than using a branch of the Big Tree.

However, for now, it has only been possible to prove that, if a Mersenne or a Fermat number is a prime, then their DiGraph contains some characteristic cycles, leading to proven PRP tests.

Theorem 11 (Lucas-Lehmer-Reix : PRP Test for Mersenne numbers). *If $M_q = 2^q - 1$ (with q prime) is a prime, then $S_{q-1} \equiv S_0 \pmod{M_q}$, with : $S_0 = 3^2 + 1/3^2$ and $S_i = S_{i-1}^2 - 2$ for $i = 1,2,3,\ldots$.*

Theorem 12 (Lucas-Lehmer-Gerbicz PRP Test for Fermat numbers). *If $F_n = 2^{2^n}+1$ is a prime, then $S_{2^n-1} \equiv S_0 \pmod{F_n}$, with : $S_0 = 1/4$ and $S_i = S_{i-1}^2 - 2$ for $i = 1,2,3,\ldots$.*

III.4 ... modulo a Wagstaff number

Since the DiGraph under x^2-2 modulo a Wagstaff number is made (proof by Michon JF, private communication) only of Cycles, it would be only possible to use a Cycle of such a DiGraph for building a Primality Proof.

Moreover, since a Wagstaff number is not smooth, it is impossible to use the Lucas-Lehmer Sequence technic (Lehmer, Ribenboim, or HC Williams) for proving that a Wagstaff number is prime. Only PRP tests are possible with such a technic.

I have experimently computed the length of the Cycles (and the number of such Cycles) of the DiGraph under x^2-2 modulo a Wagstaff number with $q \leq 31$, showing a link betwen the number of cycles of length $q-2$ and $q-1$ with irreductible polynoms (sequence A165921 of OEIS) when W_q is a prime.

See : [2] : *On different families of invariant irreducible polynomials over* $\mathbb{F}_2$, column h6 of table page 173.

Experimental data for Wagstaff numbers $q \leq 31$:

L Longueur des cycles	N Nombre de cycles de longueur L	OEIS A165921 a(L)
q=7 :		
1	2	
3	1	
5	1	1
6	1	1
q=11 :		
1	2	
3	1	
5	1	
9	9	9
10	15	15
q=13 :		
1	2	
2	1	
3	1	
4	1	
6	6	
11	31	31
12	53	53
q=17 :		
1	2	
2	1	
4	2	
5	3	
8	20	
15	363	363
16	672	672
q=19 :		
1	2	
3	2	
6	4	
9	37	
17	1285	1285
18	2407	2407
q=23 :		
1	2	
7	9	
11	124	
21	16641	16641
22	31713	31713
q=29 :		
1	4	
2	6	
3	2	
4	4	
6	1	
12	9	
14	22	
28	24	1597440
42	1	
84	2	
363	18	
726	9	
1452	9	
5082	9	
10164	198	
21665	2	
43330	8	
86660	23	
129990	18	
259980	46	
q=31 :		
1	2	
3	1	
5	6	
6	1	
10	48	
15	1454	

```
29      3085465         3085465
30      5964488         5964488
```

IV Elliptic Curves for Primality Proving

IV.1 EC for PP of Fermat numbers

In 2007-2009, 2 papers shown that it is possible to build a Primality Proof (PP) test for the Fermat numbers ($F_n = 2^{2^n}+1$) by using an Elliptic Curve (EC), following a previous paper by Benedict Gross in 2005 showing that it is possible to build a Primality Proof for Mersenne numbers using a EC.

Robert Denomme & Gordan Savin (2007-2008) : Elliptic curve primality tests for Fermat and related primes. [3]

Yu Tsumura (2009) : Primality tests for Fermat numbers and $2^{2k+1} \pm 2^{k+1} + 1$. [4]

The test by **Tsumura** (with a more generic test, using m) appears at page 7 of his paper :

$T(x) = \dfrac{x^4+2x^2+1}{4(x^3-x)}$, $x_0 = 5$, $x_{j+1} = T(x_j)$

If $x_{2^{k-1}-1} \equiv \pm 1 \pmod{F_k}$, then F_k is prime.

The test by **Denomme & Savin** appears in Chapter 4 at page 7 (or 2404) as :

$x_1 = 5$, $x_{m+1} = 1/2\left(\frac{x_m}{i} + \frac{i}{x_m}\right)$

F_n is prime iff $x_{2^k} \equiv 0 \pmod{2^{2^k}+i}$.

Though this test looks weird, and since x_{2j} is a fraction where the imaginary number i does not appear, it is possible to transform the test (expressing x_{2n} in function of $x_{2(n-1)}$) in nearly exact Tsumura's test, with a coefficient $S = \pm 1$, since $T(-x) = -T(x)$.

So, we will only consider the following EC-based Primality Test for Fermats :

Theorem 13 (Denomme/Savin - Tsumura = DST)**.**

$x_1 = F_1 = 5$, $x_{j+1} = \dfrac{x_j^4+2x_j^2+1}{4(x_j^3-x_j)}$.

If $x_{2^{n-1}} \equiv -1 \pmod{F_n}$, *then* F_n *is prime* .

IV.2 Pari/gp code for DST

(4 tests are provided. Just use the x1=... line you want to test)

```
ECPPforFermat(n,p)=
{
F=2^(2^n)+1;
if(p>0,printf("-1/3: %10d %10d\n",
      lift(Mod(-1/3,F)),-lift(Mod(1/3,F))));
x1=Mod( 5,F); iF=2^(n-1); xF=Mod(-1,F);
x1=Mod(-5,F); iF=2^(n-1); xF=Mod( 1,F);
x1=Mod( 4,F); iF=2^(n-1); xF=Mod( 0,F);
x1=Mod( 3,F); iF=2^n-1;   xF=Mod(-1/3,F);
x=x1;
for(i=2,iF,
        x=(x^4+2*x^2+1)/(4*x*(x^2-1));
        if(p==1,print(lift(x)));
);
if(p==0,print(lift(x)));
if(x == xF,
    printf("2^2^%d is prime !\n\n", n);
  , printf("2^2^%d is composite !\n\n", n); );
}
ECPPforFermat(4,1);
for(n=2,10,ECPPforFermat(n,0);print(" "));
```

IV.3 DiGraph under $\frac{x^4+2x^2+1}{4(x^3-x)}$ modulo a Fermat

The DiGraph under $\dfrac{x^4+2x^2+1}{4(x^3-x)}$ modulo a Fermat number seems (based on only the 4 known Fermat primes) to be made of :

- 3 **Big Trees** ending at : $-1, +1,$ and 0, of heigth 2^{n-1} with $2\sum_{i=0}^{n-1} 4^i$ nodes,

- plus *plenty* ($2^{n-1}+1$?) of **Cycles** of length 2^n-2 with small trees (length 1) of 4 nodes attached.

IV.3.1 Big Trees

The **first Big Tree** (ending by : -1) deals with the above proven DST Primality Test (theorem 13).

Example for $n = 4$: $\pmod{F_4}$:

$x_1 = 5 \overset{2}{\mapsto}$ -9283 $\overset{3}{\mapsto}$ 25064 $\overset{4}{\mapsto}$ -26225 $\overset{5}{\mapsto}$ -25143 $\overset{6}{\mapsto}$ -3300 $\overset{7}{\mapsto}$ 4079 $\overset{8}{\mapsto}$ **-1**

The **second Big Tree** (ending by : $+1$) is similar to the first Big Tree, with a -1 coefficient applied to all nodes.

The **third Big Tree** (ending by : 0) is associated with a candidate primality test very close to the LLT test for Mersennes (same seed 4 and same final test with 0).

Example for $n = 4$: $\pmod{F_4}$:

$x_1 = 4 \overset{2}{\mapsto}$ -4641 $\overset{3}{\mapsto}$ -14136 $\overset{4}{\mapsto}$ 17727 $\overset{5}{\mapsto}$ -5367 $\overset{6}{\mapsto}$ -10395 $\overset{7}{\mapsto}$ -256 $\overset{8}{\mapsto}$ **0**

Conjecture 2 (Denomme/Savin - Tsumura - Reix)**.**

$x_1 = \pm 4$, $x_{j+1} = \dfrac{x_j^4+2x_j^2+1}{4(x_j^3-x_j)}$.

If $x_{2^{n-1}} \equiv 0 \pmod{F_n}$, *then* F_n *is prime* .

IV.3.2 Cycles

Now, looking at the numerous Cycles of the DiGraph under $\frac{x^4+2x^2+1}{4(x^3-x)}$ modulo a Fermat number, one is special (see next section for Wagstaff numbers) and leads to the candidate PRP/Primality test for Wagstaff numbers :

Conjecture 3 (Denomme/Savin - Tsumura - Reix)**.**

$x_1 = F_0 = 3$, $x_{j+1} = \frac{x_j^4+2x_j^2+1}{4(x_j^3-x_j)}$.

If $x_{2^n-1} \equiv -1/3 \pmod{F_n}$, *then* F_n *is prime* .

(*The seed* 3 *is out of the Cycle. However this conjecture is the same as starting from* $x_1 = -1/3 \pmod{F_n}$ *and come back to it after* 2^n-2 *steps.*)

Example for $n = 3$:

$(\text{mod } F_3)$ $x_1 = 3 \overset{2}{\mapsto} 76 \overset{3}{\mapsto} 108 \overset{4}{\mapsto} 86 \overset{5}{\mapsto}$ -76 $\overset{6}{\mapsto}$ -108 $\overset{7}{\mapsto}$ -86 = **-1/3** $\mapsto 76\ldots$

Example for $n = 4$:

$(\text{mod } F_4)$ $x_1 =$ **-1/3** $= -21846 \overset{2}{\mapsto} 19116 \overset{3}{\mapsto} 5433 \overset{4}{\mapsto} 17830 \overset{5}{\mapsto} 3117 \overset{6}{\mapsto} 4769 \overset{7}{\mapsto} 23216 \overset{8}{\mapsto} 21846 \overset{9}{\mapsto}$ -19116 $\overset{10}{\mapsto}$ -5433 $\overset{11}{\mapsto}$ -17830 $\overset{12}{\mapsto}$ -3117 $\overset{13}{\mapsto}$ -4769 $\overset{14}{\mapsto}$ -23216 $\overset{15}{\mapsto}$ -21846 = **-1/3**

IV.4 EC for PP of Wagstaff numbers

IV.4.1 DiGraph under $\frac{x^4+2x^2+1}{4(x^3-x)}$ modulo a Wagstaff

Looking at the DiGraph under $\frac{x^4+2x^2+1}{4(x^3-x)}$ modulo a Wagstaff number W_q, it appears experimentaly (for the first values of q that enable to study the DiGraph : $q \leq 31$) that it is made only of Cycles of length L such that $L \mid q-2$ with 4 nodes attached to each node of each cycle.

There are always (and sometimes only) cycles of length $q-2$ and the number of these cycles is $2 \times a(q-2)$ where $a(n)$ comes from the OEIS A165921 series (irreductible polynomials).

It is noticeable that the relationship between the length of Cycles of the DiGraph modulo Wagstaff numbers and with the irreductible polynomials appears both with x^2-2 and with $\frac{x^4+2x^2+1}{4(x^3-x)}$.

Experimental data for Wagstaff numbers $q \leq 31$:

```
    L          N          OEIS
  Longueur    Nombre      A165921
des cycles  de cycles      a(L)
          de longueur L
-----------------------------------
q=7   :
     5          2            1
q=11  :
     1          2
     3          2
     9         18            9
q=13  :
    11         62           31
q=17  :
     1          1
     5          6
    15        726          363
q=19  :
    17       2570         1285
q=23  :
     1          1
     7         18
    21      33282        16641
q=29:
     1          6
     2         68
     4         72
     6         30
    12        300
   324         28
   648       8176
  1184         56
  2368        112
q=31  :
    29    6170930      3085465
```

About $q = 29$, the 6 Cycles of length 1 are : 62409100, 68475438, 175217690, 110481533, 116547871, 176629914.

Here are the Lengths and Number of cycles for 59 and 3033169 ($W_{29} = 59 * 3033169$). (N for $L \geq 6$ of 3033169 divides the corresponding N of W_{29}.)

```
    L          N
  Longueur    Nombre
des cycles  de cycles
          de longueur L
---------------------
59:
     1          2
     2          8
     4          2
3033169:
     1          2
     2          4
     4          4
     6          5
    12         20
   324          2
   648        584
  1184          4
  2368          8
```

IV.4.2 Candidate PRP test for Wagstaff numbers

Morover, looking at a specific Cycle starting at 3 and ending at $-1/3$ (same as previously seen for Fermat numbers), it appears that it is a candidate PRP test.

It has been checked that this test succeeds for all q such that W_q is known to be a prime (up to $q = 141,079$), and that it fails for all q (below 14,479) such that W_q is not a prime.

Conjecture 4 (Denomme/Savin - Tsumura - Reix = DSTR)**.**

$$x_1 = 3 \text{ or } x_1 = -1/3\ ,\ x_{j+1} = \frac{x_j^4 + 2x_j^2 + 1}{4(x_j^3 - x_j)}$$

If $x_{q-1} \equiv -1/3 \pmod{W_q}$,

then $W_q = \frac{2^q+1}{3}$ *is (PRobably) Prime .*

$q = \mathbf{7}$: $(\bmod W_7 = 43)$:

$x_1 = 3 \overset{2}{\mapsto} 10 \overset{3}{\mapsto}$ -19 $\overset{4}{\mapsto} 16 \overset{5}{\mapsto} 15 \overset{6}{\mapsto} 14 =$ **-1/3** $\mapsto 10 = x_2 \ldots$

$q = \mathbf{11}$: $(\bmod W_{11} = 683)$:

$x_1 = 3 \overset{2}{\mapsto}$ -312 $\overset{3}{\mapsto} 181 \overset{4}{\mapsto} 130 \overset{5}{\mapsto} 112 \overset{6}{\mapsto} 111 \overset{7}{\mapsto}$ -185 $\overset{8}{\mapsto} 134 \overset{9}{\mapsto}$ -65 $\overset{10=q-1}{\mapsto}$ -228 $=$ **-1/3** $\mapsto$ -312 $= x_2 \ldots$

$q = \mathbf{17}$: $(\bmod W_{17} = 43691)$:

$x_1 = 3 \overset{2}{\mapsto}$ -20024 $\overset{3}{\mapsto}$ -4673 $\overset{4}{\mapsto}$ -4921 $\overset{5}{\mapsto} 17563 \overset{6}{\mapsto}$ 12984 $\overset{7}{\mapsto}$ -5695 $\overset{8}{\mapsto} 18667 \overset{9}{\mapsto} 20891 \overset{10}{\mapsto}$ -6366 $\overset{11}{\mapsto}$ -13224 $\overset{12}{\mapsto}$ -19227 $\overset{13}{\mapsto}$ -18235 $\overset{14}{\mapsto}$ -15993 $\overset{15}{\mapsto} 511 \overset{16=q-1}{\mapsto}$ -14564 $=$ **-1/3** $\mapsto$ -20024 $= x_2 \ldots$

$q = \mathbf{19}$: $(\bmod W_{19} = 174763)$:

$x_1 = 3 \overset{2}{\mapsto} 36410 \overset{3}{\mapsto}$ -62146 $\overset{4}{\mapsto} 65849 \overset{5}{\mapsto}$ -57980 $\overset{6}{\mapsto}$ 15234 $\overset{7}{\mapsto} 76579 \overset{8}{\mapsto} 76951 \overset{9}{\mapsto}$ -1581 $\overset{10}{\mapsto} 34057 \overset{11}{\mapsto}$ 58680 $\overset{12}{\mapsto}$ -25587 $\overset{13}{\mapsto} 67892 \overset{14}{\mapsto} 66223 \overset{15}{\mapsto} 56973 \overset{16}{\mapsto}$ -77064 $\overset{17}{\mapsto} 1023 \overset{18=q-1}{\mapsto} 58254 =$ **-1/3** $\mapsto 36410 = x_2 \ldots$

$q = \mathbf{23}$: $(\bmod W_{23} = 2796203)$:

$x_1 = 3 \overset{2}{\mapsto}$ -1281592 $\overset{3}{\mapsto}$ -1066801 $\overset{4}{\mapsto}$ -896417 $\overset{5}{\mapsto}$ 973270 $\overset{6}{\mapsto}$ -1074287 $\overset{7}{\mapsto} 1341106 \overset{8}{\mapsto} 366351 \overset{9}{\mapsto}$ 333831 $\overset{10}{\mapsto} 1107490 \overset{11}{\mapsto} 937393 \overset{12}{\mapsto} 907735 \overset{13}{\mapsto}$ -1298722 $\overset{14}{\mapsto}$ -300994 $\overset{15}{\mapsto} 416316 \overset{16}{\mapsto}$ -572929 $\overset{17}{\mapsto}$ 1302116 $\overset{18}{\mapsto} 67769 \overset{19}{\mapsto}$ -1258056 $\overset{20}{\mapsto} 370787 \overset{21}{\mapsto}$ -4097 $\overset{22=q-1}{\mapsto}$ -932068 $=$ **-1/3** $\mapsto$ -1281592 $= x_2 \ldots$

$q = \mathbf{29}$: $(\bmod W_{29} = 178956971)$:

$x_1 = 3 \overset{2}{\mapsto}$ -82021944 $\overset{3}{\mapsto} 47279044 \overset{4}{\mapsto}$ -6769274 $\overset{5}{\mapsto}$ -82432991 $\overset{6}{\mapsto} 65892000 \overset{7}{\mapsto}$ -73670956 $\overset{8}{\mapsto}$ 25925635 $\overset{9}{\mapsto}$ -6570850 $\overset{10}{\mapsto} 63682155 \overset{11}{\mapsto}$ -19930570 $\overset{12}{\mapsto}$ 8768966 $\overset{13}{\mapsto}$ -80742700 $\overset{14}{\mapsto}$ -83486737 $\overset{15}{\mapsto} 60018973 \overset{16}{\mapsto}$ -89447744 $\overset{17}{\mapsto} 13157511 \overset{18}{\mapsto}$ -5229550 $\overset{19}{\mapsto}$ -51905325 $\overset{20}{\mapsto}$ -19198981 $\overset{21}{\mapsto}$ -57252499 $\overset{22}{\mapsto} 22541219 \overset{23}{\mapsto}$ 11253408 $\overset{24}{\mapsto}$ -29629532 $\overset{25}{\mapsto} 77141064 \overset{26}{\mapsto}$ -89199707 $\overset{27}{\mapsto}$ -49038102 $\overset{28=q-1}{\mapsto}$ -16133813 $\neq$ **-1/3** $(=$ 119304647) $\overset{29}{\mapsto} \ldots \overset{2370}{\mapsto} 28969859 \overset{2371}{\mapsto} 47279044 = x_3$ (Cycle of length $2368 = 2^6 \times 37$)

$q = \mathbf{31}$: $(\bmod W_{31} = 715827883)$:

$x_1 = 3 \overset{2}{\mapsto} 149130810 \overset{3}{\mapsto} 11279171 \overset{4}{\mapsto}$ -66109836 $\overset{5}{\mapsto}$ 249450180 $\overset{6}{\mapsto}$ -280431833 $\overset{7}{\mapsto}$ -97596511 $\overset{8}{\mapsto}$ -332690658 $\overset{9}{\mapsto}$ -329143902 $\overset{10}{\mapsto}$ -88687766 $\overset{11}{\mapsto}$ 324996427 $\overset{12}{\mapsto} 190514966 \overset{13}{\mapsto}$ -207459777 $\overset{14}{\mapsto}$ 131027028 $\overset{15}{\mapsto} 36447093 \overset{16}{\mapsto}$ -245289057 $\overset{17}{\mapsto}$ 199095424 $\overset{18}{\mapsto} 27348828 \overset{19}{\mapsto} 151062042 \overset{20}{\mapsto}$ 106649512 $\overset{21}{\mapsto}$ -28457251 $\overset{22}{\mapsto} 232233162 \overset{23}{\mapsto}$ 319560515 $\overset{24}{\mapsto}$ -46286542 $\overset{25}{\mapsto} 120897033 \overset{26}{\mapsto}$ 167096450 $\overset{27}{\mapsto}$ -279090714 $\overset{28}{\mapsto} 220510103 \overset{29}{\mapsto}$ 65535 $\overset{30=q-1}{\mapsto} 238609294 =$ **-1/3** $\mapsto 149130810 = x_2 \ldots$

IV.5 Pari/gp code for DSTR

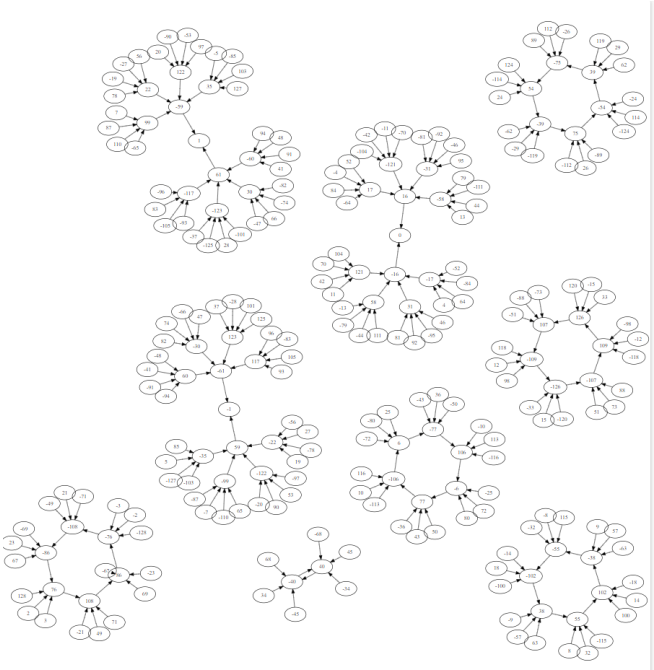
```
ECPPforWagstaff(q,p)=
{
w=(2^q+1)/3;
x1=Mod(3,w); iF=q-1; xF= Mod(-1/3,w);
x=x1;
if(p>0,print("W",q,": ",w));
if(p>1,print("-1/3: ",lift(Mod(-1/3,w))));
for(i=2,iF,
    x=(x^4+2*x^2+1)/(4*x*(x^2-1));
    if(p>0,printf("%3d %20d \n",i,lift(x))); );
if(x == xF, printf("W%d is prime ! \n", q)
    , if(p>0,printf("W%d is composite.\n", q)); );
}
ECPPforWagstaff(7,2);
ECPPforWagstaff(17,2);
forprime(q=19,15000,ECPPforWagstaff(q,0));
```

IV.6 How fast is the DSTR algorithm ?

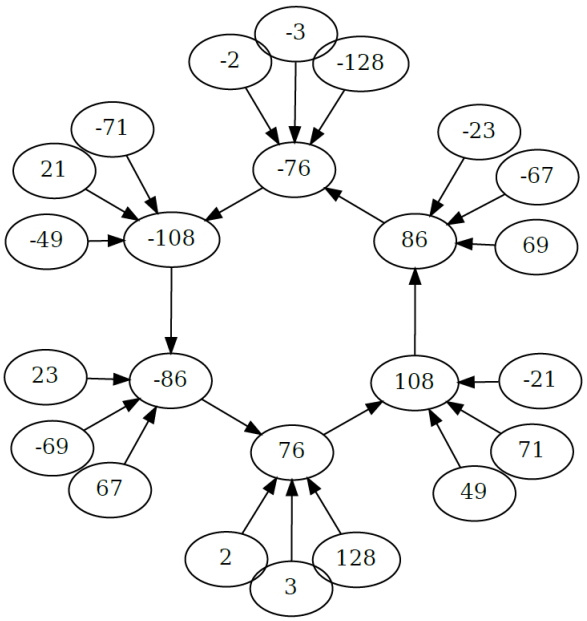
As a quick look, such a test seems to be about 5 times slower that the LLT test for Mersennes of Fermats. Thus it's still a fast test !

V Images of Digraphs under $\frac{x^4+2x^2+1}{4(x^3-x)}$ modulo ...

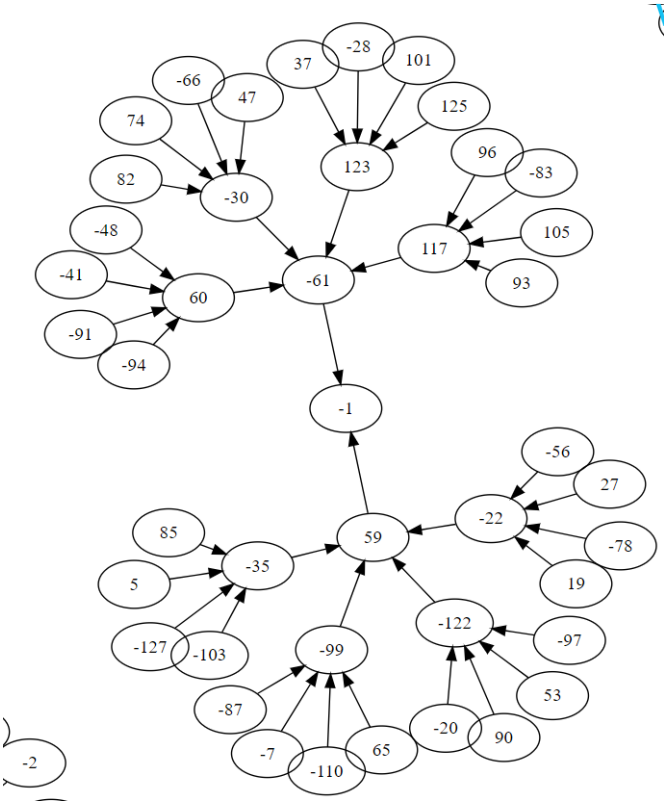
V.1 Digraph modulo Fermat F_3



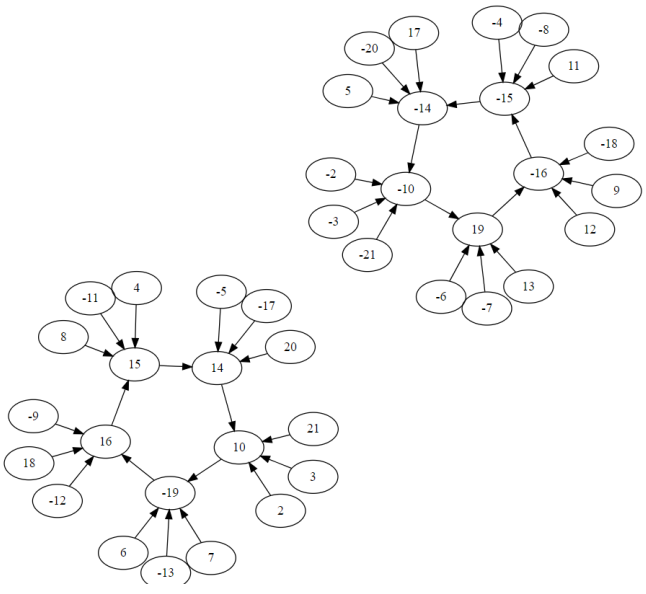
V.1.2 Cycle $x_1 = 3 \overset{2}{\mapsto}$ 76... $\mapsto$ -86 = -1/3



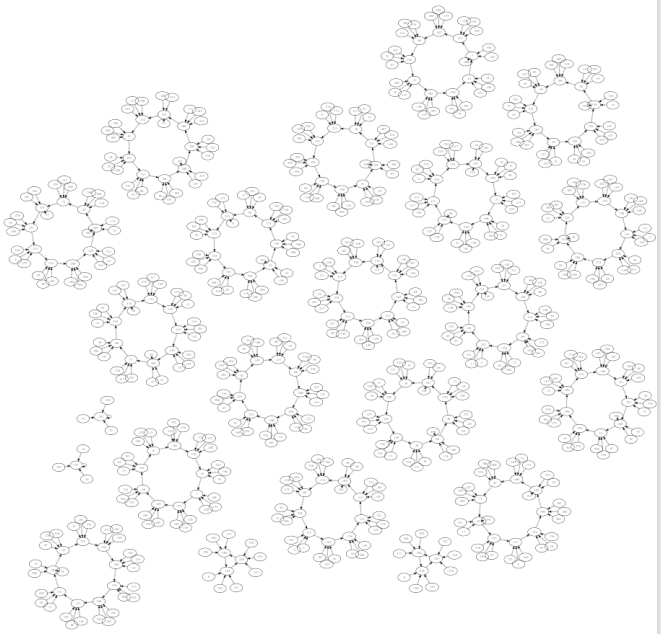
V.1.1 Big Tree $x_1 = 5 \overset{2}{\mapsto}$ -35... $\overset{8}{\mapsto}$ -1



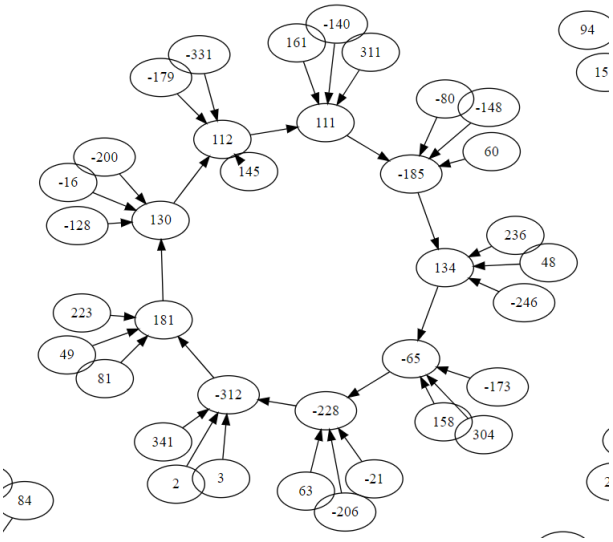
V.2 Digraph modulo Wagstaff W_7



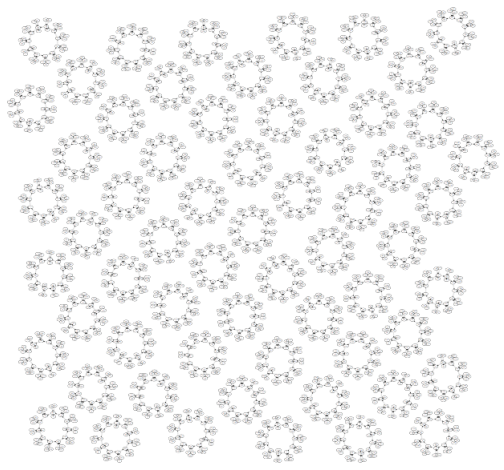
V.3 Digraph modulo Wagstaff W_{11}



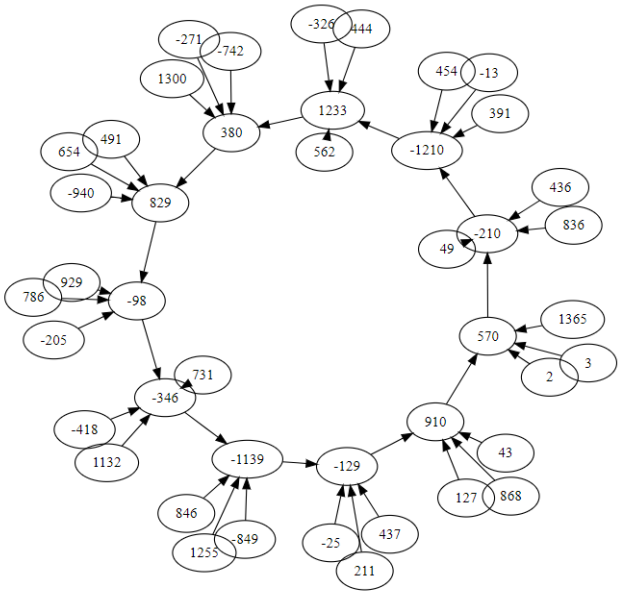
V.3.1 Cycle $3 \overset{2}{\mapsto}$ -312 $\overset{3}{\mapsto}$ ... $\overset{10=q-1}{\mapsto}$ -228 $=$ -1/3



V.4 Digraph modulo Wagstaff W_{13}



V.4.1 Cycle $3 \overset{2}{\mapsto}$ 570 $\overset{3}{\mapsto}$ ... $\overset{12=q-1}{\mapsto}$ 910 $=$ -1/3



Références

[1] T. Vasiga and J. Shallit, “On the iteration of certain quadratic maps over gf(p)”,” *Discrete Mathematics*, vol. 277, no. 1, pp. 219–240, 2004.

[2] J. F. Michon and P. Ravache, “On different families of invariant irreducible polynomials over f2,” *Finite Fields and Their Applications*, vol. 16, no. 3, pp. 163–174, 2010.

[3] R. Denomme and G. Savin, “Elliptic curve primality tests for fermat and related primes,” *Journal of Number Theory*, vol. 128, no. 1, pp. 2398–2412, 2008.

[4] Y. Tsumura, “Elliptic curve primality tests for fermat and related primes,” 2009.