Quadrature nº 42 (2024) 1-8

Les nombres de Wagstaff (v3)

Tout ce que vous avez toujours voulu savoir sur eux (sans oser demander)

par Tony REIX*

Résumé.

Après une présentation des nombres de Wagstaff, l'article rappelle les méthode connues permettant d'en trouver des PRPs (PRobably Prime) et indique le record actuel. Puis sont décrites les caractéristiques des DiGraphs (Directed Graph) générés sous x^2-2 pour les nombres de Mersenne, Fermat, et Wagstaff. On donne le lien surprenant entre le nombre de Cycles de longueur $q-1$ et $q-2$ du DiGraph sous x^2-2 modulo un nombre de Wagstaff premier et la série A165921 d'OEIS définie à partir des polynômes irréductibles. Puis on montre que le test de primalité des nombres de Fermat construit à partir de la théorie des Courbes Elliptiques semble fonctionner également pour les nombres de Wagstaff, avec de nouveau un lien surprenant entre le nombre de Cycles de longueur $q-2$ du DiGraph sous $dst(x) = \frac{x^4+2x^2+1}{4(x^3-x)}$ modulo un nombre de Wagstaff premier et la série A165921 d'OEIS.
Enfin, on fournit la visualisation de plusieurs DiGraph sous $dst(x)$ modulo des nombres de Fermat et de Wagstaff.
Le but de cet article est de susciter l'intérêt pour les nombres de Wagstaff et pour la recherche d'une méthode rapide de preuve de primalité pour ces nombres.

I Introduction

Les nombres de Wagstaff sont des cousins des nombres de Fermat et des cousins germains des nombres de Mersenne. Mais ils ne sont pas smooth comme eux... et on ne connaît donc pour le moment aucune méthode permettant de prouver **rapidement** qu'un nombre de Wagstaff est premier. On sait uniquement trouver rapidement des PRP de Wagstaff au moyen de techniques souvent inspirées du Lucas-Lehmer Test. On décrit ici une nouvelle méthode potentielle, inspirée d'un test récent de primalité pour les nombres de Fermat basé sur les Courbes Elliptiques.

II Les Nombres de Wagstaff

II.1 Définition et statut

Un nombre de Wagstaff est défini par : $W_q = \frac{2^q+1}{3}$.

W_q premier implique : q premier.

C'est aussi un RepUnit $R_n^{(b)} = \frac{b^n-1}{b-1}$ avec $b=-2$.

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

Et, avec $M_k = 2^k-1$: $W_q = 1+2M_{\frac{q-1}{2}}W_{\frac{q-1}{2}}$.

Ainsi, si q est premier, il divise soit $M_{\frac{q-1}{2}}$ soit $W_{\frac{q-1}{2}}$.

Donc, un nombre de Wagstaff n'est pas *smooth* (il ne s'écrit pas sous la forme : $W_q = N \pm 1$ où N est entièrement ou partiellement factorisé).

Il existe 34 nombres de Wagstaff premiers connus et 10 PRPs (Probably Prime) de Wagstaff. Les premières valeurs de q donnant un nombre de Wagstaff premier sont : $3,5,7,11,13,17,19,23,31,\ldots$ Le premier Wagstaff non-premier apparaît avec $q=29$. Voir la séquence

* tony.reix@laposte.net

A000978 du projet OEIS.

Actuellement, il est possible de prouver qu'un nombre de Wagstaff est premier en utilisant la méthode ECPP distribuée sur plusieurs ordinateurs. Par exemple, c'est ainsi que le nombre de Wagstaff $W_{42,737}$ (12,865 digits) a été prouvé premier par François Morain en 2007, après que je lui ai signalé que ce W_q était à portée des outils informatiques de l'époque. Le plus récent nombre de Wagstaff premier connu est $W_{127,031}$, découvert en janvier 2023.

En 2010, en tant que membre du projet DUR (Vincent Diepeveen, Paul Underwood, Tony Reix), j'ai découvert le candidat record de PRP de Wagstaff : $W_{4.031.399}$, en utilisant le test Vrba-Reix implémenté dans l'outil *LLR* par Jean Penné du projet GIMPS. Puis, au moyen de tests complémentaires, il fut prouvé comme étant un vrai PRP.

Ensuite, 3 nouveaux PRPs de Wagstaff ont été découverts, en partie en utilisant les résultats du projet DUR sur la vérification des candidats : $W_{13.347.311}$, $W_{13.372.531}$ et $W_{15.135.397}$.

II.2 Comment trouver un Wagstaff PRP

Depuis plus de 20 ans, plusieurs tests ont été trouvés et prouvés (ou conjecturés) afin de découvrir de nouveaux PRPs de Wagstaff, en utilisant plusieurs techniques (comme les séquences de Lucas ou Lehmer, utilisées pour le test LLT pour les nombres de Mersenne ou pour un test semblable au LLT pour les nombres de Fermat). Voici les principaux tests :

Theorem 1 (Lifchitz Renaud & Henri - Juillet 2000)**.** *Soit* $N_p = 2^p + 1$ *et* $W_p = \frac{N_p}{3}$ *. Si* W_p *est premier, alors on a :* $25^{2^{p-1}} \equiv 25 \pmod{N_p}$.

Theorem 2 (Vrba Anton & Reix Tony - àla LLT - Group Theory - Cycle du DiGraph)**.** *Soit* $S_{n+1} = S_n^2 - 2$ *et* p *premier* $\geqslant 3$. *Si* $W_p = \frac{2^p+1}{3}$ *est premier, alors* $S_p \equiv S_2 \pmod{W_p}$ *avec* $S_0 = 6$.

Theorem 3 (Gerbicz Robert - àla LLT)**.** *Soit* $q \geqslant 5$ *premier, et soit* $p = W(q) = \frac{2^q+1}{3}$ *un nombre premier (de Wagstaff), alors, avec la séquence* $S_0 = \frac{3}{2}$, $S_{k+1} = S_k^2 - 2$, $S_q - S_1$ *est divisible par* p .

Theorem 4 (Reix - àla Pépin - Preuve basée sur une Séquence de Lucas)**.** *Si* $W_q = \frac{2^q+1}{3}$ *(*q *premier* $\geqslant 7$*) est premier , alors on a :* $7^{\frac{W_q-1}{2}} \equiv -1 \pmod{W_q}$.

Theorem 5 (Reix - Preuve basée sur une Séquence de Lucas - Cycle du DiGraph)**.** *Si* $W_q = \frac{2^q+1}{3}$ *(*q *premier* $\geqslant 7$*) est premier, alors :* $S_q \equiv S_2 \pmod{W_q}$, *avec :* $S_0 = 8$ *et* $S_n = (S_{n-1} - 1)^2 + 1$.

Theorem 6 (Reix - àla LLT - Preuve basée sur une Séquence de Lehmer - Cycle du DiGraph)**.** *Si* $W_q = \frac{2^q+1}{3}$ *(*q *premier* $\geqslant 11$*) est premier, alors :* $S_q \equiv S_2 = 1154 \pmod{W_q}$, *avec :* $S_0 = 6$ *et* $S_i = S_{i-1}^2 - 2$ *pour* $i = 1, 2, 3, \ldots q$.

Theorem 7 (Paul Underwood - àla LLT)**.** *Si* $W_q = \frac{2^q+1}{3}$ *(*$q \equiv \pm 1 \pmod 6$*) est premier, alors :* $S_{q-2} \equiv \pm 4 \pmod{W_q}$, *avec :* $S_0 = 4$ *et* $S_i = S_{i-1}^2 - 2$ *pour* $i = 1, 2, 3, \ldots$ *et* q *premier* $\geqslant 7$.

Conjecture 1 (Reix - àla LLT - Cycle du DiGraph)**.** *Si* $W_q = \frac{2^q+1}{3}$ *(*q *premier* $\geqslant 7$*) est premier, alors :* $S_{q-1} \equiv S_0 \pmod{W_q}$, *avec :* $S_0 = 7^2 + 1/7^2$ *et* $S_i = S_{i-1}^2 - 2$ *pour* $i = 1, 2, 3, \ldots q - 1$.

III DiGraph sous $x^2 - 2$

Vasiga & Shallit ([1] : *On the iteration of certain quadratic maps over GF(p)*) ont étudié le DiGraph sous $x^2 - 2$ modulo un nombre de Mersenne ou un nombre de Fermat et ont montré que, pour chacun de ces types de nombres, leur DiGraph est constitué d'un unique Arbre Géant et de nombreux Cycles.

III.1 ... modulo un nombre de Mersenne

Le test de primalité LLT pour les nombres de Mersenne ($2^q - 1$, q premier) parcourt l'Arbre Géant du DiGraph sous $x^2 - 2$ modulo un nombre de Mersenne, en utilisant comme graine (seed) l'une des 3 graines universelles (4, 10, 2/3) et aboutissant à 0 après $q - 1$ itérations.

Theorem 8 (Test de Primalité de Lucas-Lehmer pour les nombres de Mersenne)**.** $M_q = 2^q - 1$ *(avec* q *prime) est premier ssi* $S_{q-1} \equiv 0 \pmod{M_q}$, *avec :* $S_0 = 4$ *et* $S_i = S_{i-1}^2 - 2$ *pour* $i = 1, 2, 3, \ldots$.

J'ai trouvé la formule donnant le nombre de Cycles d'un tel DiGraph sous $x^2 - 2$:

Theorem 9 (Reix - ZetaX (du forum *Art of Problem Solving*) - 2)**.** *Le nombre de Cycles de longueur L (où L divise* $q - 1 = 2^s u$*) du DiGraph* $G_{x \to x^2-2}$ *modulo un nombre de Mersenne premier* $2^q - 1$ *est :*

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

III.2 ... modulo un nombre de Fermat

Un test de primalité pour les nombres de Fermat ($F_n = 2^{2^n} + 1$) basé sur la méthode LLT utilise l'Arbre Géant du DiGraph sous $x^2 - 2$ modulo un nombre de Fermat, commençant avec la graine universelle 5 et atteignant 0 après $2^n - 2$ itérations. Il existe 4 preuves d'un test similaire pour les nombres de Fermat, le mien

inclus. On ne sait pas s'il existe d'autres graines universelles. Il est possible de prouver le test de Pépin au moyen de la technique à base d'une Séquence de Lucas-Lehmer.

Theorem 10 (Lucas-Lehmer-Reix : Test de Primalité pour les nombres de Fermat)**.**
$F_n = 2^{2^n}+1$ $(n \geq 1)$ *est premier ssi* $S_{2^n-2} \equiv 0 \pmod{F_n}$ *, avec :* $S_0 = 5$ *et* $S_i = S_{i-1}^2 - 2$ *pour* $i = 1,2,3,\ldots$.

III.3 Utilisation d'un Cycle à la place de l'Arbre Géant

On conjecture qu'il est possible de prouver qu'un nombre de Mersenne ou de Fermat est premier en utilisant un Cycle du DiGraph sous x^2-2 plutôt qu'en utilisant une branche de l'Arbre Géant du DiGraph.

Pour le moment, il a été uniquement possible de prouver que, si un nombre de Mersenne ou de Fermat est premier, alors son DiGraph présente des Cycles particuliers qui permettent de générer des tests PRP.

Theorem 11 (Lucas-Lehmer-Reix : PRP Test pour les nombres de Mersenne)**.** *Si* $M_q = 2^q - 1$ *(avec q premier) est premier, alors* $S_{q-1} \equiv S_0 \pmod{M_q}$ *, avec :* $S_0 = 3^2 + 1/3^2$ *et* $S_i = S_{i-1}^2 - 2$ *pour* $i = 1,2,3,\ldots$.

Theorem 12 (Lucas-Lehmer-Gerbicz : PRP Test pour les nombres de Fermat)**.** *Si* $F_n = 2^{2^n}+1$ *est premier, alors* $S_{2^n-1} \equiv S_0 \pmod{F_n}$ *, avec :* $S_0 = 1/4$ *et* $S_i = S_{i-1}^2 - 2$ *pour* $i = 1,2,3,\ldots$.

III.4 ... modulo un nombre de Wagstaff

Comme le DiGraph sous x^2-2 modulo un nombre de Wagstaff premier est constitué (preuve par JF Michon, communication privée) uniquement de Cycles, la seule solution possible pour construire un test de primalité consisterait à utiliser un Cycle d'un tel DiGraph.

De plus, comme un nombre de Wagstaff n'est pas smooth, il est impossible d'utiliser la technique des Séquences de Lucas-Lehmer (Lehmer, Ribenboim, ou HC Williams) pour prouver qu'un nombre de Wagstaff est premier. Avec cette technique, on ne peut construire que des tests de PRP.

J'ai calculé expérimentalement la longueur des Cycles (et le nombre de tels Cycles) du DiGraph sous x^2-2 modulo un nombre de Wagstaff avec $q \leq 31$. Ce qui a montré un lien entre le nombre de Cycles de longueur $q-2$ et $q-1$ avec les polynômes irréductibles (séquence A165961 de OEIS), quand W_q est premier.

Voir : [2] : *On different families of invariant irreducible polynomials over* $\mathbb{F}_2$, colonne h6 du tableau en page 173.

Données expérimentales pour Wagstaff $q \leq 31$:

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	4	
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 Courbes Elliptiques pour la Preuve de Primalité

IV.1 CE pour PP des nombres de Fermat

En 2007-2008, 2 articles ont démontré qu'il est possible de construire une Preuve de Primalité (PP) pour les nombres de Fermat ($F_n = 2^{2^n}+1$) en utilisant la méthode des Courbes Elliptiques (CE), faisant suite à un article de Benedict Gross en 2005 qui avait montré qu'il est possible de construite une Preuve de Primalité des nombres de Mersenne au moyen des Courbes Elliptiques.

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]

Le test prouvé par **Tsumura** (en fait un test plus générique, utilisant une variable m) apparaît à la page 7 de son article :

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

Si $x_{2^{k-1}-1} \equiv \pm 1 \pmod{F_k}$, alors F_k est premier.

Le test prouvé par **Denomme & Savin** apparaît au chapitre 4 à la page 7 (ou 2404) comme :

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

F_n est premier ssi $x_{2^k} \equiv 0 \pmod{2^{2^k}+i}$.

Bien que ce test semble assez bizarre, et parce que x_{2j} est une fraction où le nombre imaginaire i n'apparaît pas, il est possible de transformer le test (en exprimant x_{2n} en fonction de $x_{2(n-1)}$) dans une forme presque identique au test de Tsumura's, avec un coefficient $S = \pm 1$, puisque $T(-x) = -T(x)$.

Aussi, nous ne considérons içi que le test de primalité suivant :

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

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

Si $x_{2^{n-1}} \equiv -1 \pmod{F_n}$, *alors* F_n *est premier* .

IV.2 Code en Pari/gp code pour DST

4 tests différents sont fournis. Utiliser une ligne x1=... pour utiliser le test de votre choix)

```
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 sous $\frac{x^4+2x^2+1}{4(x^3-x)}$ modulo un nombre de Fermat

Le DiGraph sous $\dfrac{x^4+2x^2+1}{4(x^3-x)}$ modulo un nombre de Fermat semble (à partir des 4 seuls nombres de Fermat connus) avoir la structure suivante :

- 3 **Arbres Géants** finissant par : $-1, +1,$ ou 0, de hauteur 2^{n-1} avec $2\sum_{i=0}^{n-1} 4^i$ nœuds,

- *de nombreux* **Cycles**, dont $2^{n-1}+1$ cycles de longueur $2^n - 2$ avec de petits arbres (de longueur 1) de 3 nœuds attachés.

IV.3.1 Arbres Géants

Le **premier Arbre Géant** (finissant par : -1) est celui utilisé par le test de primalité DST ci-dessus (théorème 13).

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

$x_1 = 5 \overset{2}{\mapsto}$ -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**

Le **second Arbre Géant** (finissant par : $+1$) est similaire au premier Arbre Géant, avec un coefficient -1 appliqué à tous les nœuds.

Le **troisième Arbre Géant** (finissant par : 0) est associé à un test candidat de primalité très proche du test LLT pour les nombres de Mersenne (même graine 4 et même test final avec 0).

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

$x_1 = 4 \overset{2}{\mapsto}$ -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)**.**

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

Si $x_{2^{n-1}} \equiv 0 \pmod{F_n}$, *alors* F_n *est premier* .

IV.3.2 Cycles

Maintenant, si l'on étudie les nombreux Cycles du DiGraph sous $\dfrac{x^4+2x^2+1}{4(x^3-x)}$ modulo un nombre de Fermat, l'un d'entre eux est spécial (voir le chapitre suivant sur les nombres de Wagstaff) et laisse imaginer le test de Primalité (ou simplement PRP) pour les nombres de Wagstaff :

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

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

Si $x_{2^n-1} \equiv -1/3 \pmod{F_n}$, *alors* F_n *est premier* .

(*La graine* 3 *ne fait pas partie du Cycle. Mais cette conjecture est équivalente à partir de* $x_1 = -1/3 \pmod{F_n}$ *et y revenir après* $2^n - 2$ *étapes.*)

Example pour $n = 3$:

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

Example pour $n = 4$:

$\pmod{F_4}$ $x_1 =$ **-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 CE pour PP des nombres de Wagstaff

IV.4.1 DiGraph sous $\dfrac{x^4+2x^2+1}{4(x^3-x)}$ modulo un nombre de Wagstaff

Si l'on regarde le DiGraph sous $\dfrac{x^4+2x^2+1}{4(x^3-x)}$ modulo un nombre de Wagstaff W_q premier, il apparaît expérimentalement (pour les premières valeurs de q qui permettent d'étudier le DiGraph : $q \leq 31$) qu'il est constitué uniquement de Cycles de longeur L telle que $L \mid q-2$ avec 4 nœuds attachés à chaque nœud de chaque Cycle.

Il y a toujours (et parfois uniquement, quand $q-2$ est premier) des Cycles de longueur $q-2$; et le nombre de ces Cycles est $2 \times a(q-2)$ où $a(n)$ vient de la série A165921 d'OEIS (polynômes irréductibles).

Il est remarquable que la relation entre le nombre de Cycles du DiGraph modulo un nombre de Wagstaff et les polynômes irréductibles apparaisse à la fois avec x^2-2 et avec $\frac{x^4+2x^2+1}{4(x^3-x)}$.

Donnés expérimentales pour les Wagstaff $q \leq 31$:

L Longueur des cycles	N Nombre de cycles de longueur L	OEIS A165921 a(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

Concernant $q = 29$, les 6 Cycles de longueur 1 sont : 62409100, 68475438, 175217690, 110481533, 116547871, 176629914.

Voici les Longueur et Nombres de Cycles pour 59 et 3033169 ($W_{29} = 59 * 3033169$). (N pour $L \geq 6$ de 3033169 divise les N correspondants de W_{29}.)

L Longueur des cycles	N Nombre 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 Test PRP candidat pour les Wagstaff

De plus, en regardant un Cycle spécifique commençant à 3 et finissant à $-1/3$ (identique à ce qui a été vu pour les nombres de Fermat), il apparaît que c'est un test PRP candidat.

J'ai vérifié que ce test réussit pour tout les q tels que W_q est connu pour être premier (jusqu'à $q = 141.079$), et qu'il échoue pour tous les q (inférieurs à 14.479) tel que W_q n'est pas premier.

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

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

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

$$alors\ W_q = \tfrac{2^q+1}{3}\ est\ (PRobablement)\ Premier\ .$$

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

$x_1 = 3 \overset{2}{\mapsto} 10 \overset{3}{\mapsto}$ -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 de longueur $2368 = 2^6 \times 37$)

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

$x_1 = 3 \overset{2}{\mapsto} 149130810 \overset{3}{\mapsto} 11279171 \overset{4}{\mapsto}$ -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 Code Pari/gp pour DSTR

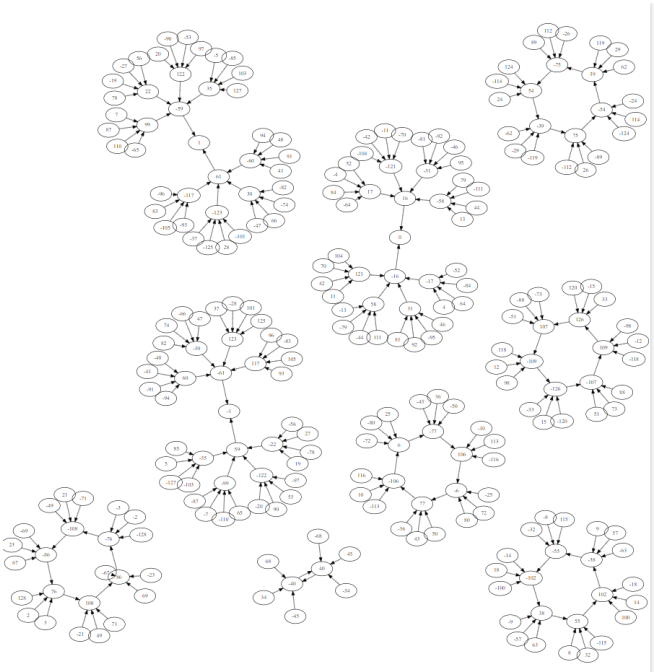
```
ECPPforWagstaff(q,p)=
{
w=(2^q+1)/3;
x1=Mod(3,w); iF=q-1; xF= Mod(-1/3,w);
x=x1;
if(p>0,print("W",q,": ",w));
if(p>1,print("-1/3: ",lift(Mod(-1/3,w))));
for(i=2,iF,
    x=(x^4+2*x^2+1)/(4*x*(x^2-1));
    if(p>0,printf("%3d %20d \n",i,lift(x))); );
if(x == xF, printf("W%d is prime ! \n", q)
    , 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 Quelle est la vitesse de l'algorithme DSTR ?

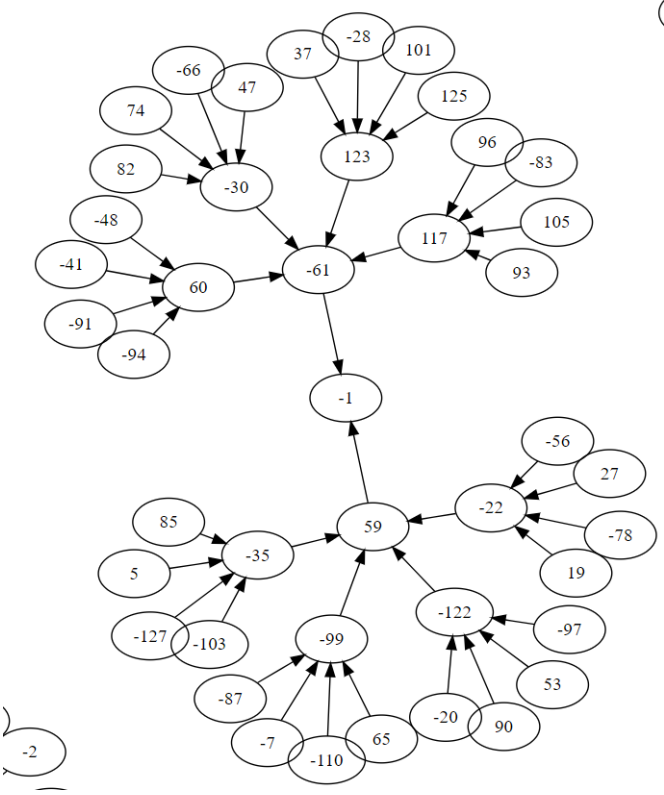
À vue de nez, ce test semble être environ 5 fois plus lent que le test LLT pour les nombres de Mersenne ou de Fermat. Ce qui reste extrêmement rapide !

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

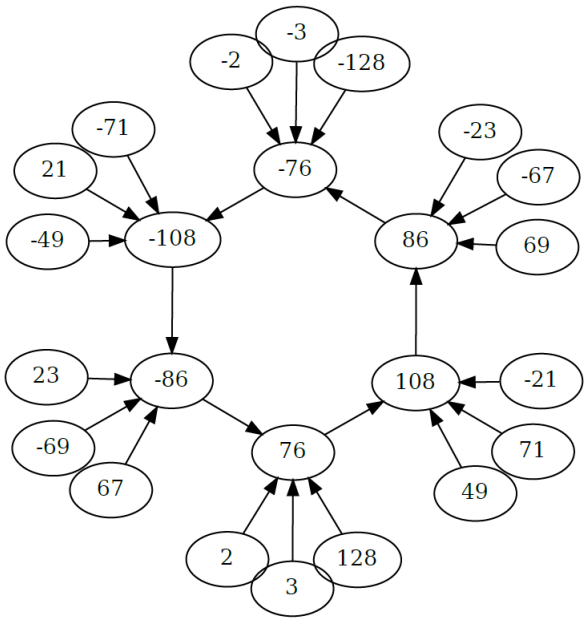
V.1 Digraph modulo Fermat F_3



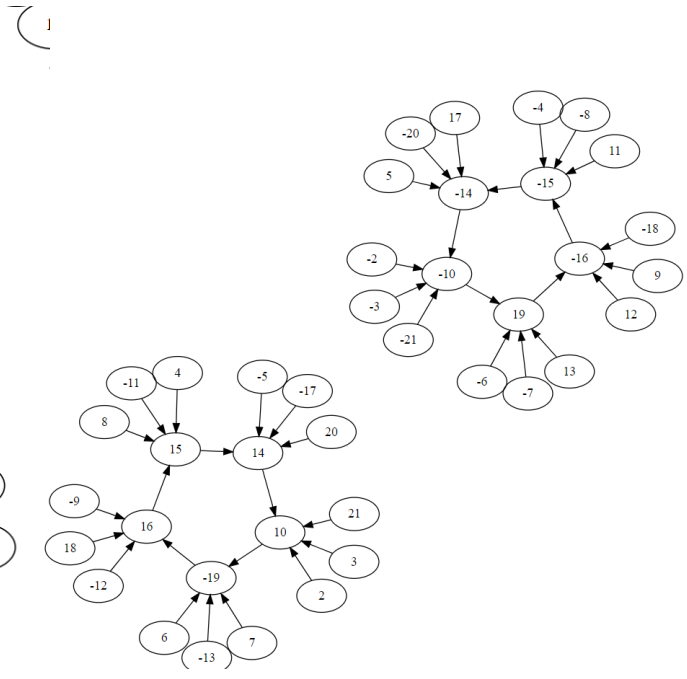
V.1.1 Arbre Géant $x_1 = 5 \overset{2}{\mapsto}$ -35... $\overset{8}{\mapsto}$ -1



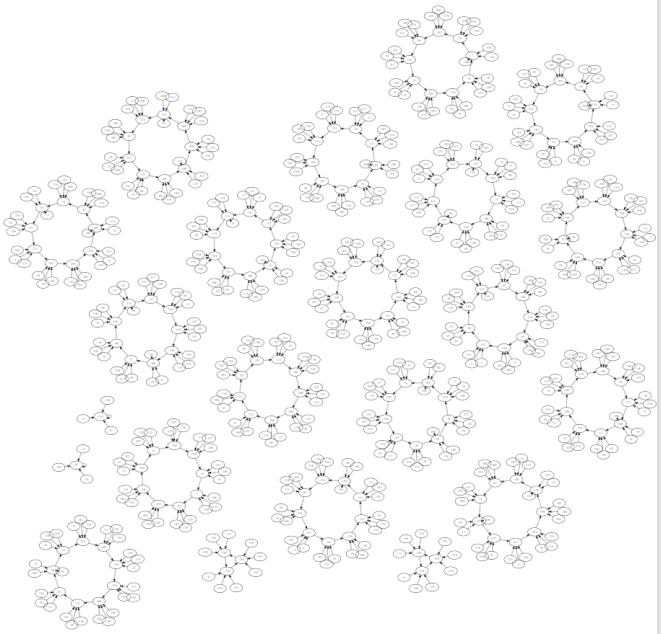
V.1.2 Cycle $x_1 = 3 \overset{2}{\mapsto}$ 76... $\mapsto$ -86 = -1/3



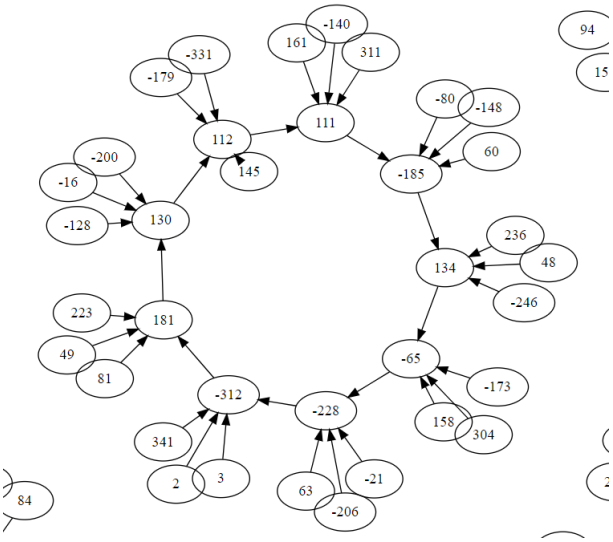
V.2 Digraph modulo Wagstaff W_7



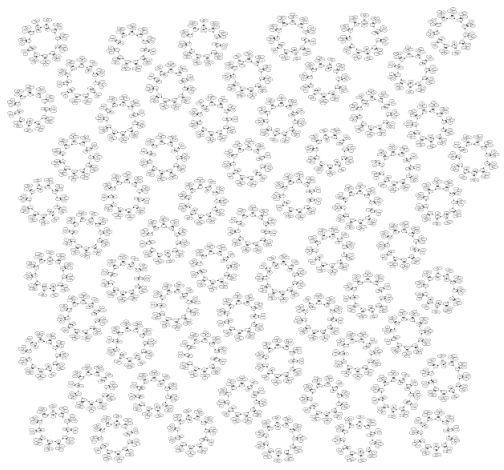
V.3 Digraph modulo Wagstaff W_{11}



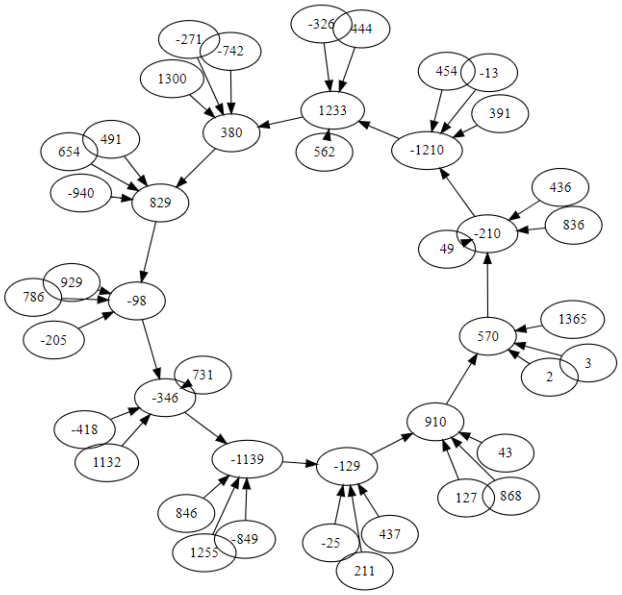
V.3.1 Cycle $3 \overset{2}{\mapsto}$ -312 $\overset{3}{\mapsto}$ ... $\overset{10=q-1}{\mapsto}$ -228 $=$ -1/3



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.