

D'UNE CONJECTURE À L'AUTRE

Cet article porte sur les itérés de nombres entiers par une fonction particulière. Comme pour le problème de Syracuse, il semble n'y avoir qu'un seul bassin d'attraction. D'où l'émergence d'une conjecture

Des outils sont créés pour la tester et voir si elle est plausible. Plusieurs facteurs limitent le champ d'investigation : la puissance de l'ordinateur, le logiciel choisi et le programme p1 qui renvoie le plus petit diviseur premier. Bien que la conjecture semble vouloir résister, elle est fautive comme le montre un contre exemple tombé du ciel.

Tout ceci est prétexte à faire de la programmation associée à des mathématiques et débouche finalement sur une autre conjecture concernant les nombres premiers jumeaux qui sera également résolue mais par une démonstration.

Sommaire

Introduction.....	page 1
Notations et définitions.....	page 1 et 2
Première partie Beaucoup de petits programmes	
Programmes.....	page 2
Itérés par la fonction.....	page 3
Constat.....	page 4
La conjecture C_1	page 4
Tests.....	page 5
Deuxième partie D'où vient le nombre 86 267 909 119 454 605	
Le paramètre c.....	page 6
Une équation intéressante.....	page 6
Recherche de solutions.....	page 7
Le nombre 86267909119454605.....	page 7
Troisième partie Une nouvelle conjecture	
La conjecture C_2	page 8
Résolution et preuves.....	page 9

Notations et définitions

Pour $n > 1$

$p1(n)$ désigne le plus petit diviseur premier de n , ainsi $p1(21) = 3$

$pap(n)$ désigne le nombre premier qui suit immédiatement $p1(n)$.

$pav(n)$ désigne le nombre premier impair (lorsqu'il existe) qui vient immédiatement avant $p1(n)$. Si $p1(n) = 3$ ce nombre n'existe pas. On pose par définition $pav(3) = 186793$ enfin si $p1(n) = 2$, $pav(n) = 0$.

La fonction f est définie sur \mathbb{N}^*

Si $n = 93396$ ou $n = 93397$ alors $f(n) = 17445812449$, sinon

$$f(n) = \frac{pav(2n + 186793)^2 + pap(|(2n - 186793)|)^2}{2}$$

Pour les deux valeurs particulières de n , $|2n - 186793| = 1$, $p1(1)$ n'est pas défini. On ne peut donc pas calculer directement l'image par la formule. L'explication du choix des nombres 186793 et 17445812449 viendra plus loin.

Première partie : Beaucoup de petits programmes.

programmes

La définition même de la fonction f implique l'usage d'un ordinateur (comment connaître le nombre premier qui suit immédiatement un nombre très grand ?). Voici trois programmes avec le logiciel Xcas qui permettent de calculer l'image d'un nombre (de 40 chiffres et plus).

Le programme principal permet d'obtenir le plus petit diviseur premier d'un entier positif différent de 0 et de 1. Dans ce programme :

Par la fonction **isprime** qui est très efficace, on teste en premier lieu si le nombre est premier.

Sinon on recherche si un petit diviseur premier (<10 000) existe. En cas d'échec,

la fonction "**ifactors**" donne la décomposition en nombres premiers avec les ordres de multiplicité.

La ligne qui suit permet de ne conserver que les diviseurs premiers dans une liste L

la fonction "**sort**" range par ordre croissant, c'est une sécurité.

Le programme renvoie le premier élément de la liste L.

```
p1(n):= {
    local K,L,x,j,l;
    x:=n ; l:=2 ;
    if(isprime(x)) {return x;}
    while(l<10000) {if(irem(x,l)==0) {return l;} l:=nextprime(l);}
    L:=NULL;
    K:=ifactors(x);
    for(j:=0;j<size(K);j:=j+2) {L:=L,K[j];}
    return sort(L)[0];} ;
```

Ce programme manque parfois d'efficacité pour certains grands nombres. Notamment lorsque la recherche d'un petit diviseur échoue. Cela peut venir du fait qu'on demande par la fonction "**ifactors**" tous les facteurs du nombre alors que seul le plus petit nous intéresse.

Les deux autres programmes en découlent.

Le premier utilise la fonction **nextprime** de Xcas qui donne le nombre premier qui suit immédiatement.

```
pap(n) :={
    return nextprime(p1(n));
} ::
```

De fait $\text{pap}(n) := \text{nextprime}(p1(n))$.

Il en va autrement pour la fonction "pav" qui n'est pas simplement $\text{prevprime}(p1(n))$. Les multiples de 2 et de 3 y sont traités différemment.

```
pav(n) :={
    local x ;
    x:=p1(n) ;
    if(x==2){return 0;}
    if(x==3){return 186793;}
    return prevprime(x);
} ::
```

Le programme pour la fonction f s'écrit alors facilement

```
f(n):= {
    local x;
    x:=n;
    if(x==93397){return 17445812449;}
    if(x==93396){return 17445812449;}
    return ( pav(2x+186793)2 + pap(abs(2x-186793))2 )/2;
} ::
```

la fonction "abs" est la valeur absolue.

La ligne de commande : `for(l:=1;l<10;l++){afficher(f(l));}` donne les images des huit premiers nombres.

n	1	2	3	4	5	6	7	8
f(n)	17445812509	73	17445824749	17445824749	64453	65	17445812605	25

Itérés par la fonction

il faut maintenant créer un programme qui permette d'observer les premiers itérés par f. Dans ce programme la variable k désigne le nombre d'itérations de n par f. Le résultat est donné sous forme d'une liste L dont les éléments sont les itérés successifs.

```
F(n,k):={
    local x,c,L;
    c:=0; x:=n; L:=n;
    while(c<k){x:=f(x); L:=L,x; c:=c+1;}
    L;} ::
```

Par exemple : le résultat pour $F(2,5)$ est

2, 73, 34864737025, 17445812485, 17445812689, 17445812449

73 est le premier itéré de 2, 17445812449 le cinquième.

La ligne de commande `for(l:=1;l<9;l++){afficher(F(l,5));}` permet d'obtenir les cinq premiers itérés des huit premiers nombres

```
1,17445812509,17445812449,17445812449,17445812449,17445812449
2,73,34864737025,17445812485,17445812689,17445812449
3,17445824749,17445812449,17445812449,17445812449,17445812449
4,17445812449,17445812449,17445812449,17445812449,17445812449
5,64453,17445818365,608706639719448963829,17445812449,17445812449
6,65,37,17445812569,17445812449,17445812449
7,17445812605,17445812509,17445812449,17445812449,17445812449
8,25,34884900949,17445812449,17445812449,17445812449
```

Constat

Le nombre 17445812449 attire l'attention.

C' est un point fixe , il est sa propre image.

Il est attractif, les images successives par f aboutissent à ce nombre.

Remarque

Dans la définition de f pour les nombres 93396 et 96397, on a choisi ce nombre pour rester dans le bassin d'attraction.

Par la commande citée plus haut on peut tout aussi facilement obtenir les 5 premiers itérés des cent- un premiers nombres. Quelques nombres n'aboutissent pas à 17445812449 mais en augmentant le nombre d'itérations, tous aboutissent. Exemple pour 11.

```
11,17,157,34833394105,17445812485,17445812689,17445812449,17445812449,17445812449
```

Ainsi se pose la question : pour toute valeur de n la suite des itérés par f finit elle par atteindre le nombre 17445812449 ? C'est la conjecture C_1 .

Pour tout n la suite des itérés de n par f aboutit à 17445812449 C_1

Pour rendre plausible la conjecture il faut plus qu'une centaine de valeurs. Faisons un programme qui permette de tester un grand nombre de valeurs.

Pour n donné le programme suivant renvoie 1 si la suite des itérés de longueur 20 atteint 17445812449, il renvoie 0 sinon..

```
test(n):={
    local x,c;
    c:=0 ; x:=n;
    while(c<20){x:=f(x);
    if( x==17445812449){return 1;}
    c:=c+1; }
    return 0; } ;;
```

Par la ligne de commande qui suit, on teste si parmi les entiers inférieurs à 1000, on en trouve un dont la suite des itérés de longueur 20 n'atteint pas 17445812449. Pour un ordinateur peu puissant, il faut moins de dix secondes pour tester les 1000 premiers nombres.

Voici la réponse de Xcas :

```
for(j:=1;j<1000;j++){if(test(j,20) !=1){return j;};}
```

Evaluation time: 9.578

0

La réponse 0 signifie que l'ordinateur n'en a pas trouvé. Il n'en trouve pas non plus parmi les nombres inférieurs à 100 000. Voici les temps indicatifs par tranche de 10 000.

tranche	0 – m	m -2m	2m -3m	3m -4m	4m -5m	5m -6m	6m -7m	7m -8m	8m -9m	9m.....
temps	65 s	67 s	66 s	66 s	67 s	66 s	67 s	66 s	66 s	64 s

Le temps varie beaucoup en fonction de la puissance de l'ordinateur. En présence de plusieurs ordinateurs et en répartissant les tâches on accélère la recherche..

Remarque

La régularité des temps est étonnante, on ne rencontre pas de factorisation difficile bien que les nombres manipulés soient parfois grands. Par exemple pour le nombre 54947.. Le quatrième itéré est : $x = 1801545450353056932217811112126345913591455076317128321861394057782839378387534201211185,$

Le calcul du cinquième itéré est facilité par la recherche préliminaire d'un petit diviseur qui trouve rapidement '97 ce qui évite de calculer la factorisation complète de $2x-186793$ qui est

[97,1,179,1,491,1,59021,1,5864198830309,1,1158748848070861811,1,1053815047442434659853399301086285618299285811,1].

Avant 1000 000 aucun contre exemple n'est trouvé. La recherche peut se poursuivre jusqu'à

Malgré tout, seuls une démonstration ou un contre exemple peuvent résoudre la conjecture C_1 .

Le nombre 86267909119454605 sorti, comme le lapin, du chapeau d'un prestidigitateur met fin à la recherche car $f(86267909119454605) = 86267909119454605$

La conjecture C_1 est fausse

Il y a probablement entre 1000 000 et ce nombre d'autres nombres qui réfutent la conjecture C_1 .

Quel est le plus petit ? Est il proche de 1000 000 ? D'autres logiciels permettent ils de le trouver plus facilement ?.....

Deuxième partie : D'où vient le nombre 86267909119454605?

L'étude des points fixes d'une famille de fonctions permet de le découvrir.

Le paramètre c

La définition de la fonction f repose sur le nombre 186793, on peut le remplacer par un paramètre c impair et congru à 1 modulo 3 c à d de la forme $6k + 1$. La fonction "pav" retourne alors le paramètre c, à la place de 186793 lorsque $p1(n) = 3$.

```
pav(n,c):= {
    local x ;
    x:=p1(n) ;
    if(x==2){ return 0;}
    if(x==3){ return c;}
    return prevprime(x) ;} ;;
```

Les valeurs pour lesquelles on ne peut pas calculer l'image par la formule sont $\frac{c-1}{2}$ et $\frac{c+1}{2}$

On crée provisoirement deux points fixes singuliers, qu'on peut éventuellement modifier une fois la valeur de c déterminée (comme cela est fait pour la fonction f dans la première partie). On obtient

```
f(n,c):= {
    local x;
    x:=n;
    if(x==(c-1)/2){return (c-1)/2;}
    if(x==(c+1)/2){return (c+1)/2;}
    return ( pav(2x + c,c)^2 + pap(abs(2x - c))^2 )/2;}
};;
```

Une équation intéressante $q = pap(q^2 + c^2 - c)$

q désigne un nombre premier et c de la forme $6k + 1$

Si (c,q) est une solution de l'équation $q = pap(q^2 + c^2 - c)$ alors le nombre $n = \frac{c^2 + q^2}{2}$ est un point fixe pour f(n,c).

Soit $n = \frac{c^2 + q^2}{2}$, si (c, q) est solution de l'équation, q qui est le suivant d'un nombre premier

impair est supérieur à 3 donc 3 divise $q^2 + c^2 + c = 2n + c$. On en déduit $pav(2n + c) = c$.

Comme

$$pap(2n - c) = q \text{ par définition de la fonction on a } f(n, c) = \frac{c^2 + q^2}{2} . .$$

Remarque

On peut montrer que tous les points fixes non singuliers sont de la forme $\frac{c^2 + q^2}{2}$ pour un certain nombre premier q. Il existe cependant une exception lorsque $c = 1 + 30k$ car alors 17 est un point fixe et il n'est pas de la forme $\frac{c^2 + q^2}{2}$.

Recherche de solutions

En rapport avec cette équation on pose $p = p_1(q^2 + c^2 - c)$, q est le nombre premier qui suit immédiatement p , posons $q = p + h$.

p est donc un diviseur de $(p+h)^2 + c^2 - c$ et finalement p divise $h^2 + c^2 - c$.

Pour c donné et h fixé le nombre $h^2 + c^2 - c$ est déterminé, on peut connaître ses diviseurs premiers et sélectionner ceux qui éventuellement donnent des points fixes.

Détail des étapes

On commence par établir une liste T des valeurs possibles du paramètre

"Pour chacune de ces valeurs "ce qui dans la ligne de commande se traduit par

```
j:=0;while(j<size(T)){c:=T[j]
```

"On considère les diviseurs premiers impairs de $h^2 + c^2 - c$ "

```
K:=ifactors( h^2+c^2-c );for(l:=2;l<size(K);l:=l+2)).
```

"Puis on sélectionne les couples (c,q) qui donnent un point fixe."

```
if(nextprime(K[l])==K[l]+h && p1((K[l]+h)^2 + c^2 - c )==K[l])
```

```
{afficher(c,K[l]+h);}j:=j+1;}
```

Exemple le nombre 86267909119454605.

Les valeurs du paramètre c sont des nombres premiers de la forme $30t + 13$.

```
T:=NULL;;t:=0;;while(t<10000){if(isprime(30*t+13)!=0){T:=T,30*t+13;}t:=t+1;};T;
```

Pour $h = 6$, on sélectionne les candidats en fonction des valeurs de c .

```
j:=0;while(j<size(T)){y:=T[j];K:=ifactors(y^2-y+36);for(l:=2;l<size(K);l:=l+2)
```

```
{if(nextprime(K[l])==K[l]+6 && p1((K[l]+6)^2+y*(y-1))==K[l]){afficher(y,K[l]+6);}j:=j+1;
```

Un extrait de la réponse de Xcas.

182773,59

184993,79

185833,29

186793,415374269

187123,7649

187393,89

187573,29

D'où le point fixe

$$\frac{186793^2 + 415374269^2}{2} = 86267909119454605$$

Troisième partie Une nouvelle conjecture

Un cas intéressant surgit lorsque $h = 2$ à d quand p et q sont des nombres premiers jumeaux .
Par exemple pour T définie par

```
T:=NULL.;t:=0.;while(t<10000){T:=T,6t+1;t:=t++;};T;
```

La ligne de commande suivante

```
j:=0;while(j<size(T)){c:=T[j];K:=ifactors(c^2-c+4);for(l:=2;l<size(K);l:=l+2){if(isprime(K[l]+2)!=0 && p1((K[l]+2)^2+c*(c-1))==K[l]){afficher(c,K[l]+2)
```

donne une réponse assez longue dont voici un extrait.

```
13,7
43,7
55,1489
73,7
91,19
97,19
.....
59869,19
59893,7
59923,7
59935,109
59953,7
59965,19
Evaluation time: 91.156
```

Le premier cas trouvé (13, 7) signifie que si on attribue la valeur 13 au paramètre c , $109 = (13^2 + 7^2) / 2$ est point fixe.
L'examen de la liste en son entier montre que les couples jumeaux(p , q) sont
Soit (5, 7)
Pour les valeurs de c 13, 43, 73, 103.....
.....
soit de la forme ($10k + 7$, $10k + 9$)
Pour 55, 91, 97.....
Est ce une simple présomption ? En est il toujours ainsi ?

Il est assez facile de montrer que pour $h = 2$, le couple ($30t + 13$, 7) est solution de l'équation des points fixes.

Pour la deuxième constatation : le chiffre des unités de q est 9 .lorsque p est différent de 5, on peut tenter un énoncé assez simple et plus général.

Conjecture C_2 .

Si [p , $p+2$] est un couple de nombres premiers jumeaux différent des couples (3,5) et (5, 7) et si p divise $n^2 - n + 4$ pour un certain entier n alors le chiffre des unités de p est 7.

Il est intéressant de créer différents programmes pour tester C_2 , cependant aucun contre exemple n'est trouvé. Se pose alors la question : Une démonstration existe t elle ?

Résolution de C_2

Remarque préliminaire

Si $(p, p + 2)$ est un couple de nombres premiers jumeaux différent de $(3, 5)$ et $(5, 7)$ alors p a pour chiffres des unités 1, 7 ou 9.

La démonstration de C_2 découle facilement des deux propositions suivantes

* Si un nombre premier p est congru à 1 modulo 10 et divise $n^2 - n + 4$ pour une certaine valeur de n alors p est de la forme $30t + 1$.

** Si un nombre premier p est congru à 9 modulo 10 et divise $n^2 - n + 4$ pour une certaine valeur de n alors p est de la forme $30t + 19$.

Pour chacune de ces propositions on constate que 3 divise $p + 2$ donc $(p, p + 2)$ n'est pas un couple de jumeaux

Ce qui résout la conjecture C_2 car le chiffre des unités de p ne peut être ni 1, ni 9. C'est donc 7.

Preuve des propositions

p premier divise $n^2 - n + 4$ s'écrit $n^2 - n + 4 - py = 0$ pour un certain nombre entier y .

L'équation obtenue est une équation diophantienne que l'on peut mettre sous la forme

$$(2n-1)^2 - p(4y) = -15.$$

le nombre -15 est congru à un carré modulo p . Il est donc résidu quadratique modulo p

En utilisant le symbole de Legendre cela équivaut à $\left(\frac{-15}{p}\right) = 1$ c'est à dire $\left(\frac{-3}{p}\right)\left(\frac{5}{p}\right) = 1$
(propriété du symbole de Legendre)

Les deux résultats suivants semblent être établis depuis plusieurs siècles

- p congru à 1 modulo 3 équivaut à -3 est un carré modulo p .
- p congru à ± 1 modulo 5 équivaut à 5 est un carré modulo p .

Donc -15 est résidu quadratique modulo p dans quatre cas

$$\text{deux pour } \left(\frac{-3}{p}\right) = 1 \text{ et } \left(\frac{5}{p}\right) = 1$$

1)- p congru à 1 modulo 3 et p congru à 1 modulo 5 c à d p de la forme $30t + 1$ (car p est impair).

2)- p congru à 1 modulo 3 et p congru à 4 modulo 5 c à d p de la forme $30t + 19$. "

$$\text{deux pour } \left(\frac{-3}{p}\right) = -1 \text{ et } \left(\frac{5}{p}\right) = -1$$

3)- p congru à 2 modulo 3 et p congru à 2 modulo 5 c à d p de la forme $30t + 17$. "

4)- p congru à 2 modulo 3 et p congru à 3 modulo 5 c à d p de la forme $30t + 23$. "

Ce qui démontre les deux propositions du haut de la page.