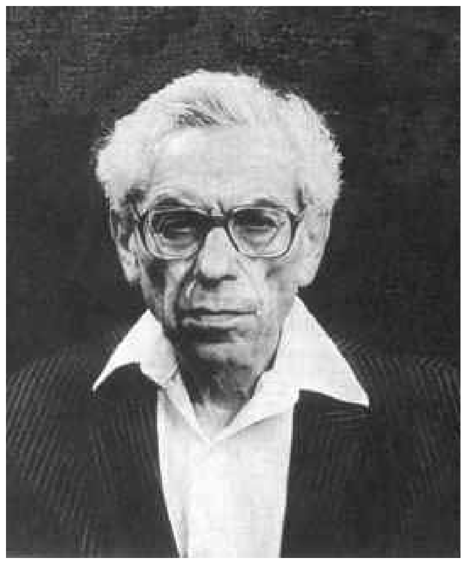
# La conjecture d'Erdös et Straus

groupe EXPRIME

Lyon 2009



.

**Préliminaires**.

En Février 2009, une étudiante en Master nous expose son projet de mémoire qui concerne la conjecture dite d'Erdös-Straus que ces deux auteurs ont formulée en 1948.
Celle-ci est une des généralisations de la décomposition $1 = \frac{1}{2} + \frac{1}{3} + \frac{1}{6}$.
Cette conjecture s'énonce ainsi :
« Pour tout entier n plus grand que 1, $\frac{4}{n}$ est somme de trois fractions égyptiennes. »
A ce jour elle n'est pas encore démontrée, même si d'une part elle est vérifiée pour tout nombre plus petit que $10^{14}$ et si elle est démontrée pour de nombreuses classes de nombres.
L'objectif de cette présentation de la conjecture d'Erdös-Straus est de montrer (démontrer ! ?) que, via l'utilisation du concept d'entier pythagoricien, cette conjecture est valide.

# 1 - Quelques résultats partiels

1. Si $n$ vérifie la conjecture alors $k\,n$ également, car si : $\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ alors : $\frac{4}{k\,n} = \frac{1}{k\,x} + \frac{1}{k\,y} + \frac{1}{k\,z}$. Ainsi tout multiple d'un nombre premier vérifiant la conjecture la vérifie aussi.
   Conséquence : comme $\frac{4}{2} = 2 = 1 + \frac{1}{2} + \frac{1}{2}$ alors $\frac{4}{2\,n} = \frac{1}{n} + \frac{1}{2\,n} + \frac{1}{2\,n}$.
   Autrement dit, tout nombre pair vérifie la conjecture.
   De même tout multiple de 3 vérifie la conjecture car $\frac{4}{3} = 1 + \frac{1}{4} + \frac{1}{12}$, ou tout multiple de 5 ($\frac{4}{5} = \frac{1}{2} + \frac{1}{4} + \frac{1}{20}$) ou tout multiple de 7 ($\frac{4}{7} = \frac{1}{2} + \frac{1}{15} + \frac{1}{210}$), etc.
   Mais comment trouver une décomposition générique pour tout nombre premier ?

2. Une autre approche : on a l'identité : $\frac{4}{2+3\times x} = \frac{1}{1+x} + \frac{1}{2+3\times x} + \frac{1}{(1+x)\times(2+3\times x)}$, autrement dit tout nombre égal à 2 modulo 3 vérifie la conjecture. Si l'on établit suffisamment d'autres identités de ce type, $\frac{4}{P(x)} = \frac{1}{P_1(x)} + \frac{1}{P_2(x)} + \frac{1}{P_3(x)}$ où $P$, $P_1$, $P_2$ et $P_3$ sont des polynômes, on peut espérer prouver la conjecture.

3. Une troisième approche pour résoudre $\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ est de prendre pour $\frac{1}{x}$ la plus grande fraction égyptienne plus petite que $\frac{4}{n}$ puis pour $\frac{1}{y}$, la plus grande fraction égyptienne plus petite que $\frac{4}{n} - \frac{1}{x}$ enfin de voir sous quelles conditions $\frac{4}{n} - \frac{1}{x} - \frac{1}{y}$ est une fraction égyptienne $\frac{1}{z}$. Eh bien cette approche marche pas mal puisqu'on a le résultat suivant :
   si $n$ modulo 24 est différent de 1 et de 17, alors cette méthode marche. Voici l'algorithme associé :

```
> Erdös3:=proc(n)
> local x,y,z;
> if  not(n mod 24 #n mod 12=3,7 et 11 {1,17}) then x:=trunc(n/4)+1;
  y:=trunc((1/(4/n-1/x)))+1;z:=1/(4/n-1/x-1/y); return([4/n=[1/x,1/y,1/z]]) fi:
> #c'est la solution standard avec x minimum possible E(n/4)+1.
> #il reste les nombres congrus à 1 et 17 à étudier
> #pour 17 on utilise le fait que n modulo 3 = 2 (le polynôme ci-dessus) :
> if n mod 24 =17 then return([4/n=[3/(n+1),1/n,3/n/(n+1)],17]) fi:
> return([n,'modulo 24=',1]):
> end:
> [seq(Erdös3(2*m+1),m=1..15)];
        [[4/3 = [1, 1/4, 1/12]], [4/5 = [1/2, 1/4, 1/20]],
        [4/7 = [1/2, 1/15, 1/210]], [4/9 = [1/3, 1/10, 1/90]],
        [4/11 = [1/3, 1/34, 1/1122]], [4/13 = [1/4, 1/18, 1/468]],
        [4/15 = [1/4, 1/61, 1/3660]], [4/17 = [1/6, 1/17, 1/102], 17],
        [4/19 = [1/5, 1/96, 1/9120]], [4/21 = [1/6, 1/43, 1/1806]],
        [4/23 = [1/6, 1/139, 1/19182]], [25, modulo 24=, 1],
        [4/27 = [1/7, 1/190, 1/35910]], [4/29 = [1/8, 1/78, 1/9048]],
        [4/31 = [1/8, 1/249, 1/61752]]]
```

Cet algorithme est simple et très rapide. Je pensais que la preuve dépassait le cadre de cet exposé ; en fait non, voir en annexe une preuve élémentaire, trouvée après la mise au point de pas mal d'algorithmes.

4. Encore une autre approche, c'est celle qui consiste à écrire $\frac{4}{n}$ comme somme de deux fractions égyptiennes et d'en déduire une décomposition en somme de trois fractions en coupant en deux une des fractions obtenues.
   Cette méthode peu utilisée est cependant intéressante car on a un algorithme qui nous donne les nombres entiers tels que $\frac{4}{n} = \frac{1}{x} + \frac{1}{y}$ et qui montre bien les difficultés pour résoudre la conjecture d'Erdös-Straus.

Terminons ces préliminaires en signalant que dès l'énoncé de cette conjecture en 1948, il y a eu pas mal de travaux sur le problème plus général visant à établir une décomposition en somme de trois fractions égyptiennes pour les rationnels $\frac{a}{b}$, avec $a < b$, avec en particulier la conjecture de Sierpinski qui affirme la véracité de cette décomposition pour les fractions de la forme $\frac{5}{n}$.

## 2 - Sur les entiers tels que $\frac{4}{n}$ soit somme de deux fractions égyptiennes

Évidemment tout entier ne peut s'écrire comme somme de deux fractions égyptiennes, autrement cela se saurait, au moins comme conjecture.
De fait environ 90% des entiers s'écrivent sous une telle forme.
Étudier cet ensemble d'entiers m'a paru comme un préliminaire pour saisir la profondeur des difficultés pour prouver la conjecture d'Erdös-Straus et des concepts mis en œuvre, en particulier celui de nombre pythagoricien (i.e. de la forme 4n+1 ou encore somme de deux carrés).
Après de multiples procédures (avec un logiciel de calcul formel) et des consultations de pages de l'encyclopédie des suites "Sloane", voici deux procédures d'une part assez efficaces et d'autre part proches d'une démonstration avec papier et crayon.

1. Pour tous les entiers : où les entiers de la forme $4m \pm 1$ sont mis en évidence
   Après des premiers programmes de balayages (lents) puis de tests (nettement plus rapides et contrôlés par les précédents) voici un algorithme :

```
Erdös2c:=proc(n)#un autre programme théorique avec ajout de tests
> local x,y,k,a,pa,ra,na;
> if n+1 mod 4=0 then k:=(n+1)/4:x:=k*n:y:=k:#n mod 12 dans {3,7,11}
> return([4/n,k,1/x,1/y,‘4m-1‘]):fi:
> if n mod 2=0 or n mod 12=9 then
> x:=trunc(n/4)+1;y:=(1/(4/n-1/x)); return([4/n=[1/x,1/y],1,standard]) fi:
> #c’est la solution standard avec x minimum possible E(n/4)+1.
> #il reste les nombres congrus à 1 et 5 modulo 12 à étudier
```

```
> #avec les premiers de la forme 4k-1
> #programme théorique qui est inutile pour les nombres premiers
> for a from 2 to trunc(n/48)+1 do
> if isprime(4*a-1) then
> #a parcourt les entiers tels que 4a-1 soit un premier
> pa:=4*a-1;#ra:=12*pa;na:=n mod ra;#na donne les restes possibles mod 12*pa
> if n mod pa=0 then x:=trunc(n/4)+a;y:=(1/(4/n-1/x));#ou if na mod pa=0 ...
> return([4/n=[1/x,1/y],a,pa,n mod (12*pa)]) fi;# ou na
> fi;od;#return([n,‘ pas de solution‘]);
> end:
> w:=time():test2:=[seq(Erdös2c(2*m+1),m=2..50000)]:time()-w;nops(test2);
                                52.034
                                40377
test2[30..45];
 [[4/87, 22, 1/1914, 1/22, ‘4m-1‘],
 [4/91, 23, 1/2093, 1/23, ‘4m-1‘],
 [4/93 = [1/24, 1/744], 1, standard],
 [4/95, 24, 1/2280, 1/24, ‘4m-1‘],
 [4/99, 25, 1/2475, 1/25, ‘4m-1‘],
 [4/103, 26, 1/2678, 1/26, ‘4m-1‘],
 [4/105 = [1/27, 1/945], 1, standard],
 [4/107, 27, 1/2889, 1/27, ‘4m-1‘],
 [4/111, 28, 1/3108, 1/28, ‘4m-1‘],
 [4/115, 29, 1/3335, 1/29, ‘4m-1‘],
 [4/117 = [1/30, 1/1170], 1, standard],
 [4/119, 30, 1/3570, 1/30, ‘4m-1‘],
 [4/121 = [1/33, 1/363], 3, 11, 121],
 [4/123, 31, 1/3813, 1/31, ‘4m-1‘],
 [4/127, 32, 1/4064, 1/32, ‘4m-1‘],
 [4/129 = [1/33, 1/1419], 1, standard]]
```

Remarques :

- le pgcd de 6 (tout nombre premier $> 3$ est égal à $\pm 1$ modulo 6) et de 4 (les nombres pythagoriciens ou non sont égaux à $\pm 1$ modulo 4) est 12, nombre qui revient de manière importante dans ce problème.
- voici la suite des premiers nombres $n$ tels que $\frac{4}{n}$ n'admet pas de décomposition en somme de deux fractions égyptiennes : 5, 13, 17, 25, 29, 37, 41, 53, 61, 65, 73, 85, 89, 97, 101, 109, 113, 125, 137, 145, 149, 157, 169, 173, 181, 185, 193, 197 ; ils sont tous de la forme 4m+1 ; mais surtout ce sont les premiers pythagoriciens ou des produits de ceux-ci, voir Sloane A008846.
- dans la dernière partie du programme $na$ donne les restes possibles modulo $12 \times pa$, il y en a très peu ; par exemple pour a=3, $pa$=11, $na$=77 ou 121 (ou $n$ modulo

132=77 ou 121). Présenté ainsi cet algorithme est proche de la preuve ; on peut en déduire un algorithme plus rapide, mais qui cachera les points clefs.

– il est à noter que, contrairement à la méthode standard qui cherche $x$ le plus petit possible, l'utilisation des nombres de la forme $4m-1$ permet de chercher un $x$ multiple de $n$ (le plus petit possible) d'où $y$ est « petit ».
  De plus cette méthode à l'avantage de moins utiliser la partie entière d'un nombre, ce qui rend plus efficace les procédures mises en œuvre.
  Attention, lorsque que l'on cherche $x$ de la forme $x = kn$, le plus petit possible, $k$ peut être grand : par exemple pour $n = 2999$ (et $n = 13 \times 2999^2$), $k = 750$.

2. Pour les premiers, seuls ceux qui sont de la forme $4m-1$ admettent une décomposition en somme de deux fractions égyptiennes ; cela doit sûrement être connu, même si ce résultat n'a pas beaucoup d'intérêt en lui-même, il est significatif pour avancer dans la compréhension de la conjecture d'Erdös-Straus. L'algorithme pour les nombres premiers se réduit alors aux trois premières lignes du précédent :

```
Erdös2e:=proc(n)#pour les nombres premiers:
> local x,y,k;
> if n+1 mod 4=0 and isprime(n) then k:=(n+1)/4:x:=k*n:y:=k:
  #n modulo 4=3 et n premier
> return([4/n,k,1/x,1/y,‘m-1‘]):fi:
> end:
```

# 3 - Sur la conjecture d'Erdös-Straus

Où en est-on ? Pour $\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ , il est établi que :

Premier résultat : on sait déterminer des solutions de cette équation pour tous les nombres différents de : 1, $11^2$, $13^2$, $17^2$, $19^2$, $23^2$ modulo 840 par une certaine méthode. Ces solutions $x(n)$, $y(n)$ et $z(n)$ sont polynomiales en $n$.
Référence : Mordell L.J, Diophantine equations, London, New York : Academic press, 1969, chapter 30.

Second résultat : pour les nombres congrus à 1, $11^2$, $13^2$, $17^2$, $19^2$ et $23^2$ modulo 840, Alain Schinzel a montré que ces solutions n'étaient pas polynomiales en $n$.
Référence : Schinzel A. On sums of three unit fractions with polynomial denominators. Funct. Approx. Comment. Math. 28 :187-194, 2000.

Nous allons développer une étude en s'appuyant, non pas sur cette classification modulo 840, mais sur les nombres de la forme $4m-1$ et de propriétés des nombres premiers modulo 12.
Heuristique : si l'on a une solution $\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$, avec $x = f(n)$ ; $y = g(n, x)$ alors on n'a pas forcément une solution $\frac{4}{n} = \frac{1}{y} + \frac{1}{x} + \frac{1}{z}$ (où $y = f(n)$ et $x = g(n, y)$) et inversement.
Par ailleurs, la solution standard qui marche dans la plupart des cas, s'appuie sur le fait que $x$ est le plus petit entier possible tel que $\frac{1}{n} - \frac{1}{x}$ soit positif, idem pour $y$, d'où l'entier

$z$ est très très grand (de l'ordre de $n^4$, cf. annexe, lemme 1).
Du fait des (très) nombreuses solutions possibles, l'idée développée est de chercher des $x$ multiple de $n$, donc pas très petit, tels que l'on obtienne une solution ; de fait souvent $y$ est plus petit que $x$ et $z$ n'est pas astronomique (de l'ordre de $n^2$).
Ça marche ; après avoir établi différents algorithmes, toujours de plus en plus « efficaces », je me suis attaché à établir des algorithmes plus proches d'une démonstration théorique (avec papier et crayon) ; certes légèrement plus lents, ces algorithmes reposent en définitive sur l'utilisation de la nature pythagoricienne ou non d'un nombre premier (disons plutôt de la forme $4m \pm 1$).

En tout cas, ma connaissance de propriétés des nombres premiers modulo 24, puis modulo 12, (840 est un nombre incongru égal à $5 \times 7 \times 24$) m'a beaucoup servi pour élaborer ces algorithmes, merci à M. Parmentier, un vendeur d'oeufs et fromages, qui m'a transmis ses travaux à propos du calcul modulo 24. Sans doute à l'avenir des chemins de preuves plus esthétiques seront trouvés. Pour moi, suivant l'école chinoise d'il y a plus de deux mille ans ou l'école babylonienne d'il y a 4000 ans, l'algorithme marche, donc il faut accepter l'axiome algorithmique (dit parfois maintenant axiome de l'ordinateur) au même titre que l'axiome du choix. C'est très constructiviste mais bougrement efficace. D'un point de vue épistémologique, n'est-il pas souvent démontré des résultats du type « sous l'hypothèse de Riemann, on a ... » ou « si la conjecture d'Erdös-Straus est valide on a .. », n'est-ce pas implicitement accepter cet axiome algorithmique chinois ou babylonien ?

Ingrédients :

- pour les premiers $p$ de la forme $4m-1$ on utilise le résultat de la décomposition de $p$ en deux fractions et le fait que pour tout $k$ on a $\frac{1}{k} = \frac{1}{k+1} + \frac{1}{k(k+1)}$, ce qui donne : $x = k \times p$, $y = k+1$ et $z = k \times (k+1)$ où $k = \frac{p+1}{4}$.
- tous les nombres premiers plus grands que 3 sont égaux à 1, 5, 7, 11 modulo 12 (à 1, 5, 7, 11, 13, 17, 19 et 23 modulo 24) et les premiers non pythagoriciens sont égaux à 7 et 11 modulo 12 (à 7, 11, 19 et 23 modulo 24). Après la mise au point des algorithmes en utilisant le calcul modulo 24, les propriétés des nombres premiers modulo 12 suffisent, ce qui corrobore l'algorithme du § précédent et la pertinence de l'introduction des nombres de la forme $4m-1$.
- pour les premiers égaux à 5 modulo 12 (ou à 5 et 17 modulo 24), on utilise le fait que $p$ modulo 3=2, et donc $x = p$ , $y = \frac{p+1}{3}$ et $z = p \times y$ donne une décomposition de $\frac{4}{p}$.
- il ne reste plus, pour résoudre la conjecture, qu'à trouver un algorithme pour les premiers égaux à 1 modulo 12 (ou à 1 et 13 modulo 24). Évidemment, si l'on tient compte de tous les résultats obtenus aujourd'hui, il suffirait de montrer que pour les nombres premiers égaux à 1, 121, 169, 289, 381 et 529 modulo 840 on a une solution, mais on sait que c'est une entreprise quasi impossible.
  Aussi notre approche, profondément différente, s'est servie cependant de ces résultats pour tester les algorithmes successifs mis au point.
- pour $p = 1$ modulo 12, on utilise d'abord le fait que si, par exemple, $p$ modulo 7

$(7 = 4 \times 2 - 1)$ est dans $T_2 = 3, 5, 6$ alors $x = 2p$, $y = E\left(\frac{x}{7}\right) + 1$ et $z = \dfrac{1}{\frac{4}{p} - \frac{1}{x} - \frac{1}{y}}$ fournit une solution ; et plus généralement pour $m$, si $p$ mod $(4m-1)$ est dans $T_m$ $x = mp$, $y = E\left(\frac{x}{4m-1}\right) + 1$ et $z = \dfrac{1}{\frac{4}{p} - \frac{1}{x} - \frac{1}{y}}$ est solution. Voir le lemme 2 en annexe.

Tout repose sur les nombres premiers qui ne sont pas égaux à 3 modulo 4. Prenons un exemple d'utilisation de cette propriété : 13 n'est pas de la forme $4m - 1$ ; certes il existe des multiples de 13 qui le sont, comme $39 = 3 \times 13 = 40 - 1$.
C'est cette propriété (valide pour tout premier de la forme $4m + 1$) qui sous-tend l'algorithme proposé qui permet de valider la conjecture d'Erdös-Straus.
C'est l'heuristique de la preuve.
D'où l'algorithme théorique suivant obtenu après une dizaine d'autres ; évidemment il existe des versions plus performantes de cet algorithme, toujours basées sur ces principes, mais plus loin de l'heuristique mise en œuvre.
On construit d'abord le tableau TT sur la base du lemme 2 :

```
construitT:=proc(m)
> local p,b,k,x,y,z,A,t,tt,u;
> p:=(4*m-1)*k+b:x:=m*p;y:=m*k+1+trunc(m*b/(4*m-1));
> z:=p*y*m/((4*m-1)*(1+trunc(m/(4*m-1)*b))-m*b);
> A:=[seq([u,eval(subs(b=u,z))],u=0..(4*m-2))]:
> t:=select(u->denom(op(2,u))=1,A):
> tt:=convert(map(u->op(1,u),t),set);return(tt);
> end:
> TT:=[seq(constructT(i),i=1..2000)]:#8mn environ pour 2000, 2mn pour 1000
> TT[1..6];
  [{0, 2}, {0, 3, 5, 6}, {0, 7, 8, 10},
   {0, 3, 5, 6, 7, 10, 11, 12, 13, 14}, {0, 15, 18},
   {0, 7, 10, 11, 15, 19, 20, 21, 22}]
```

puis on écrit le programme proprement dit :

```
> Erdos3cinque:=proc(p) #vers la preuve pour les nombres impairs
> local x,y,z,k,b,c,m;
> global TT;
> if p+1 mod 4=0 then k:=(p+1)/4:x:=k*p:y:=k+1:z:=k*(k+1):
> return([p,k,[x,y,z]]):fi: #pour p mod 12=7, 11
> if p mod 3=2 then x:=p:y:=(p+1)/3:z:=p*y:
> return([p,1,[x,y,z],bis]):fi:#pour p mod 12=5
> #il reste les nombres égaux à 1 mod 12
> for m from 2 to 2000 do
> if p mod (4*m-1) in TT[m] then x:=m*p:y:=trunc(x/(4*m-1))+1:z:=1/(4/p-1/x-1/y):
> return([p,m,[x,y,z],ter]):
```

```
> fi:od:
> for m from 2001 to (p+1)/4 do #il n'y a aucune raison de borner m
> #pour les rares restants :
> x:=m*p:y:=trunc(x/(4*m-1))+1:z:=1/(4/p-1/x-1/y):
> if is(z,integer) then return([p,m,[x,y,z],cinque]):fi:
> od:
> return([p,echec]);
> end:
> G:=[seq(ithprime(i),i=1..100000)]:nops(G);
                                100000
> w:=time():test:=map(u->Erdos3cinque(u),G):time()-w;test[1..20];nops(test);
                                8.763
  [[2, 1, [2, 1, 2], bis], [3, 1, [3, 2, 2]], [5, 1, [5, 2, 10], bis],
        [7, 2, [14, 3, 6]], [11, 3, [33, 4, 12]],
        [13, 2, [26, 4, 52], ter], [17, 1, [17, 6, 102], bis],
        [19, 5, [95, 6, 30]], [23, 6, [138, 7, 42]],
        [29, 1, [29, 10, 290], bis], [31, 8, [248, 9, 72]],
        [37, 4, [148, 10, 740], ter], [41, 1, [41, 14, 574], bis],
        [43, 11, [473, 12, 132]], [47, 12, [564, 13, 156]],
        [53, 1, [53, 18, 954], bis], [59, 15, [885, 16, 240]],
        [61, 2, [122, 18, 549], ter], [67, 17, [1139, 18, 306]],
        [71, 18, [1278, 19, 342]]]
                                100000
> P:=select(u->nops(u)=3,test):nops(%);#pour p modulo 12=7 ou 11
                               50050
> Pbis:=select(u->nops(u)=4 and op(4,u)=bis,test):nops(%);#pour p modulo 12=5
                               25012
> Pter:=select(u->nops(u)=4 and op(4,u)=ter,test):nops(%);#pour p modulo 12=1
                               24938
> Pcinque:=select(u->nops(u)=4 and op(4,u)=cinque,test):nops(%);
                                 0
#il n'y a pas d'exceptions;
```

Que reste-t-il à prouver (de manière bourbakiste) pour montrer que l'algorithme est juste ?

1 - que les restes possibles modulo les nombres $4m-1$ (inférieurs à 2000 dans l'algorithme ci-dessus) sont corrects. Voir le lemme 2 en annexe.

2 - il faut montrer que forcément on a une solution à partir de ces nombres, (inférieurs à 2000 ci-dessus), et de leurs multiples (bornés par $p/4$) ; là c'est plus délicat car c'est un théorème d'existence. Voir corollaire 2 en annexe. Ce corollaire montre qu'il y a un nombre « négligeable » de nombres qui sont susceptibles de ne pas vérifier la conjecture, il ne démontre pas encore celle-ci ; il faudrait pour cela établir un lemme de majoration du type par exemple, dans les notations du lemme 2 et du corollaire 2 : pour tout premier $p = p_n$ (i.e. le n-ième nombre premier) il existe $q = q_m$ premier,

$q \leq p$, tel que p ne soit pas dans $R_m$.

Remarques :

- cet algorithme est adapté aux nombres premiers et en particulier à ceux égaux à 1 modulo 12, c'est le sens de l'extension « cinque » donné au nom de la procédure (qui succède à une précédente nommée quarte mais plus loin de la preuve). Cette procédure ne donne pas seulement la décomposition en somme de trois fractions égyptiennes de $\frac{4}{n}$, mais la valeur du paramètre $m$, conduisant à cette décomposition.
- dans cet algorithme, j'ai borné le paramètre $m$ du tableau TT à 2000 ; pour augmenter l'efficacité algorithmique, on peut entrer un tableau TT avec :
  $m \leq 210 = 7\times5\times3\times2$, ce qui augmente les « exceptions » (de fait avec $m \leq 210$, pour tous les premiers égaux à 1 modulo 12 et inférieurs à $10^8$, il n'y a aucune exception).
- il y aurait beaucoup d'autres remarques à faire ; une dernière. Il est à noter que cette méthode conduit à une décomposition $\frac{4}{p} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ telle que $y \leq x$ et surtout avec $z$ « petit », i.e. $z \sim p^2$, ce qui est très différent de la méthode utilisée usuellement qui conduit à des $z$ « astronomiques » de l'ordre de $p^4$.

# 4 - Sur la conjecture de Sierpinski

C'est en écrivant des éléments de preuve, avec papier et crayon, que je me suis aperçu que les algorithmes mis en jeu marchaient très bien, modulo des modifications évidentes, pour étudier la conjecture de Sierpinski : pour tout $n \geq 5$ la fraction $\frac{5}{n}$ est somme de trois fractions égyptiennes ; et plus généralement pour examiner le problème de la décomposition en somme de trois fractions égyptiennes des rationnels $\frac{a}{b}$. Alors en bref, voici la procédure mise en œuvre, qui utilise la construction décrite en annexe au §III :

```
> Ta:=[seq(construitTa(i,5),i=1..400)]:# pour a=5
> Sierpinski:=proc(p,a)
> local x,y,z,m,k;
> global Ta;
> for m from 1 to 400 do
> if p mod (a*m-1) in Ta[m] then x:=m*p:y:=trunc(x/(a*m-1))+1:z:=1/(a/p-1/x-1/y):
> return([a/p,m,[1/x,1/y,1/z],bon]):
> fi:od:
> for m from 401 to (p+1)/4 do #pour les rares restants :
> x:=m*p:y:=trunc(x/(a*m-1))+1:z:=1/(a/p-1/x-1/y):
> if is(z,integer) then return([a/p,m,[1/x,1/y,1/z],bon1]):fi:
> od:
> return([p,‘echec‘]);
> end:
```

Cet algorithme est valide pour a quelconque, en mettant sa valeur dans le tableau Ta des restes donnant lieu à une décomposition. Mais cet algorithme est limité aux nombres premiers, ce qui est l'essentiel pour établir des résultats.

Pour les 100000 premiers nombres premiers $p > 5$, **toutes** les fractions $\frac{5}{p}$ sont décomposées en somme de trois fractions égyptiennes en quelques secondes.
Pour $a = 6$ et 7, cette procédure décompose toutes les fractions $\frac{6}{p}$ et $\frac{7}{p}$, pour les 100000 premiers nombres premiers, toujours en quelques secondes, à l'exception de quelques petits nombres premiers : pour $a = 6$, les nombres 61, 73, 397, 457, 601, 613, 1093, 2521 et 84673 ; pour $a = 7$, les nombres 43, 127, 211, 421, 463, 631 et 12601.

Pour $a$ compris entre 8 et 13, les exceptions sont un peu plus nombreuses, cependant de plus en plus rares lorsque $p$ augmente, ce qui laisse à penser que le corollaire 2 en annexe est valide, mutatis mutandis, pour tout $a$, i.e. pour toutes les fractions rationnelles.

**Remarque conclusive :**

Pour moi la conjecture d'Erdös-Straus est résolue d'un point de vue algorithmique et la preuve formelle va reposer essentiellement sur l'utilisation des premiers de la forme $4m-1$.
Et pour en revenir aux décompositions en somme de fractions égyptiennes de rationnels, cet exemple montre, une fois de plus, à quel point la connaissance des nombres premiers est intimement liée à celle de ces décompositions.
Une narration de recherche au fil des jours (et d'algorithmes)
Michel, Vaulx-en-Velin, Avril 2009.

# 5 - Annexe : éléments de preuves

**I - sur les restes modulo 24**

Soit $p$ un nombre premier de la forme $p = 24k + b$ ; les restes possibles $b$ sont 1, 5, 7, 11, 13, 17, 19 et 23. Posons $x = E\left(\frac{p}{4}\right) + 1$, $y = E\left(\frac{1}{\frac{p}{4} - \frac{1}{x}}\right) + 1$ et $z = \frac{1}{\frac{p}{4} - \frac{1}{x} - \frac{1}{y}}$ ; on obtient alors avec les paramètres $k$ et $b$ : $x = 6k + 1 + E(\frac{b}{4})$, c'est à dire un polynôme en $k$, avec des coefficients dépendant de $E\left(\frac{b}{4}\right)$. Pour $y$ on obtient un polynôme de degré 2 en $k$, et pour $z$ un polynôme de degré 4. Il reste à voir pour quelles valeurs de $b$ ces polynômes sont à coefficients entiers. On obtient :

**Lemme 1** : Soit $p = 24k + b$, alors pour $b$ différents de 1 et de 17, $z$ est un polynôme en $k$ à coefficients entiers. En particulier pour $b = 1$, 5, 7, 11, 13, 17, 19 et 23, ces polynômes, de degré 4, sont les suivants :

- pour $b = 1$, $z_1 = 1/2 \times (24k + 1) \times (6k + 1) \times (48k^2 + 10k + 1)$, jamais entier
- pour $b = 5$, $z_5 = 2 \times (24k + 5) \times (3k + 1) \times (24k^2 + 13k + 2)$, entier
- pour $b = 7$, $z_7 = 6 \times (24k + 7) \times (3k + 1) \times (48k^2 + 30k + 5)$, entier
- pour $b = 11$, $z_{11} = 6 \times (24k + 11) \times (2k + 1) \times (72k^2 + 69k + 17)$, entier
- pour $b = 13$, $z_{13} = 2 \times (24k + 13) \times (3k + 2) \times (24k^2 + 29k + 9)$, entier
- pour $b = 17$, $z_{17} = 1/2 \times (24k + 17) \times (6k + 5) \times (48k^2 + 74k + 29)$, jamais entier
- pour $b = 19$, $z_{19} = 6 \times (24k + 19) \times (6k + 5) \times (24k^2 + 39k + 16)$, entier
- pour $b = 23$, $z_{23} = 6 \times (24k + 23) \times (k + 1) \times (144k^2 + 282k + 139)$, entier

La preuve est élémentaire, mais un peu fastidieuse ; elle justifie l'algorithme *Erdös3* présenté. On notera que $z$ est forcément un grand nombre de l'ordre de $p^4$. Comme 17=2 modulo 3, il ne reste plus qu'à montrer que pour $p = 1$ *modulo* 24, la conjecture de Erdös est valide ce qui va présenter quelques difficultés.

**II - sur les restes modulo** $4m-1$

**Lemme 2 :** soit $p = (4m-1)k + b$, où $m$ est un entier positif et $b$ le reste de la division euclidienne de $p$ par $4m-1$. Posons $x = mp$, $y = E\,(p/4) + 1 = mk + 1 + E\left(\frac{mb}{4m-1}\right)$ et $z = \dfrac{pym}{(4m-1) \times \left(1 + E\left(\frac{mb}{4m-1}\right) - mb\right)}$ ; alors :

i) si pour $b$, $z$ est un polynôme en $k$ à coefficients entiers, il est de degré 2 et $\frac{4}{p} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ est une décomposition en une somme de trois fractions égyptiennes.

ii) Notons $T(m)$ l'ensemble des $b$ tels que $z$ soit un polynôme en $k$ à coefficients entiers, alors 0, $4m-2$ et $4m-5$ appartiennent à $T(m)$ (pour $m > 1$).

La preuve, du même type que celle du lemme précédent pour i) justifiant ainsi l'algorithme utilisé, est donc élémentaire ; cependant nous allons donner les polynômes obtenus pour montrer ii), car ce point entraîne une conséquence importante sur l'existence d'une décomposition. Un petit calcul montre que si $p = (4m-1)k + 4m - 2$, alors $x = mp$, $y = m(k+1)$ et $z = m(k+1)\left((4m-1)k + 4m - 2\right)$ ; et si $p = (4m-1)k + 4m - 5$, alors $x = mp$, $y = m(k+1) - 1$ et $z = \left(m(k+1) - 1\right)\left((4m-1)k + 4m - 5\right)$.

Il est facile de montrer que $T(1) = 0, 2$, $T(2) = 0, 3, 5, 6$, $T(3) = 0, 7, 8, 10$, $T(4) = 0, 3, 5, 6, 7, 10, 11, 12, 13, 14$, $T(5) = 0, 15, 18$, etc. .

Conséquences : avec l'utilisation du lemme chinois.

**Corollaire 1 :** Pour tout $p$ différent de 1, 121, 169, 289, 361 et 529 modulo 840, il existe une décomposition de $\frac{4}{p}$ en somme de trois fractions égyptiennes.

D'après le lemme 1, il reste à étudier les nombres égaux à 1 modulo 24, en particulier ceux égaux à 1 modulo 8 ; D'après le lemme 2, en utilisant T(2) il reste à étudier les nombres égaux à 1, 2 et 4 modulo 7. Le lemme chinois nous dit qu'il reste à étudier les nombres égaux à 1, 9 et 25 modulo $56 = 7 \times 8$. L'utilisation de T(5) nous dit qu'il reste à étudier les nombres égaux à 1, 2, 4, 8 et 9 modulo 15. Le lemme chinois nous donne 15 restes possibles modulo $840 = 15 \times 56$. Appliquons le lemme 1 en sélectionnant les restes égaux à 1 modulo 24, ce sont les nombres 1, 121, 169, 289, 361 et 529. On a ainsi démontré par des moyens élémentaires le résultat bien connu (cf. Mordell, 1969). Il y a cependant deux différences : premièrement les décompositions associées à $p$ sont différentes ; la méthode classique donne en général un $z$ de l'ordre de $p^4$, alors que cette méthode donne en général un $z$ de l'ordre de $p^2$. Deuxièmement on peut itérer le processus en considérant T(3), ce qui nous donne 42 restes possibles modulo $9240 = 11 \times 840$, puis avec les ensembles T(m) du lemme 2.

**Corollaire 2 :** Notons $n!$ la factorielle première, c'est à dire le produit des $n$ premiers nombres premiers, puis $K_n = 4 \times n!$ et $R_n$ l'ensemble des restes à étudier modulo $K_n$, suivant la méthode initialisée au corollaire précédent alors :

$$\lim_{n\to\infty} \frac{Card(R_n)}{K_n} = 0,$$

Ce résultat est une amélioration importante du corollaire précédent. Construisons d'Abord par récurrence l'ensemble $R_n$. Soit $p$ le n+unième nombre premier de deux choses l'une, soit $p$ est de la forme $4m-1$ et $R_{n+1}$ s'obtient par le lemme chinois à partir de $R_n$ et de T(m) (du moins son complémentaire dans les $4m-1$ premiers entiers), soit $p$ est différent de $4m-1$, alors $3p$ est de la forme $4m-1$. Dans ce cas on applique le lemme chinois à partir de T(m) et de $R_n$ *modulo* $K_n/3$ puis on sélectionne les restes qui conviennent (dans $R_n$ modulo $K_n$) pour obtenir $R_{n+1}$. On applique alors le lemme 2 ii) qui permet la majoration : $\frac{Card(R_{n+1})}{K_{n+1}} \leq \frac{4m-4}{4m-1}\frac{Card(R_n)}{K_n}$. cqfd. Par exemple $\frac{Card(R_5)}{K_5} = 6/840 \approx 0,007$ et $\frac{Card(R_6)}{K_6} = 42/9240 \approx 0,0045$, ce qui signifie qu'il y a très peu (et de moins en moins) de nombres premiers qui échappent à la conjecture d'Erdös-Straus.

### III - sur les restes modulo $a\,m-1$

**Lemme 3 :** Soit la fraction $\frac{a}{p}$, soit m un entier plus grand que 1 et soit $p=(am-1)k+b$, la division euclidienne de $p$ par $a\,m-1$ ; posons $x = mp$, $y = mk+1+E(\frac{mb}{am-1})$ et $z = \dfrac{pym}{(am-1)\times(1+E(\frac{mb}{am-1})-mb)}$ ; de la même manière que précédemment, si pour $b$, $z$ est un polynôme en $k$ à coefficients entiers, ce polynôme est de degré 2 et on obtient la décomposition en somme de trois fractions égyptiennes $\frac{a}{p}=\frac{1}{x}+\frac{1}{y}+\frac{1}{z}$.
Voici un programme qui permet d'obtenir rapidement ces restes possibles pour tout $a$ et $m$.

```
> construitTa:=proc(m,a)
> local p,b,k,x,y,z,A,t,tt,u;
> p:=(a*m-1)*k+b:x:=m*p;y:=m*k+1+trunc(m*b/(a*m-1));
> z:=p*y*m/((a*m-1)*(1+trunc(m/(a*m-1)*b))-m*b);
> A:=[seq([u,eval(subs(b=u,z))],u=0..(a*m-2))]:
> t:=select(u->denom(op(2,u))=1,A):
> tt:=convert(map(u->op(1,u),t),set);return(tt);
> end:
> construitTa(2,4);construitTa(2,5);construitTa(2,7);
                        {0, 3, 5, 6}
                     {0, 3, 4, 6, 7, 8}
                       {0, 6, 11, 12}
> seq(construitTa(i,6),i=1..6);
  {0, 4}, {0, 5, 9, 10}, {0, 11, 14, 16}, {0, 11, 17, 19, 21, 22}, {0, 23, 24, 28},
  {0, 5, 7, 10, 11, 14, 15, 16, 17, 20, 21, 23, 28, 29, 30, 32, 33, 34}
```