Sur la conjecture d'Erdös et Straus

Michel Mizony

Vaulx-en-Velin 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 des entiers de la forme $4m - 1$, cette conjecture est valide.

En effet l'approche standard de ce problème consiste à prendre la plus grande fraction égyptienne plus petite que $\dfrac{4}{n}$, puis de recommencer, ce qui nécessite le recours à la fonction « partie entière » à plusieurs niveaux.
Mon but a été d'emblée d'aborder cette conjecture en essayant de me passer de cette fonction « partie entière ».
Le résultat principal de cette contribution est effectivement de donner une (des) méthode(s) algorithmique(s) qui reste(nt) dans le cadre de la théorie des nombres (donc qui se passe de la fonction analytique « partie entière ») et, de fait, qui améliore considérablement les résultats partiels trouvés à ce jour.
Ce résultat principal peut s'énoncer ainsi : soit p un nombre premier, s'il existe un entier positif m et un diviseur d de m^2 tels que $p + 4d$ soit divisible par $4\,m - 1$, alors $\dfrac{4}{p}$ est somme de trois fractions égyptiennes. De plus la plupart des résultats partiels connus se ramènent à cette propriété qui entraîne ipso facto celle d'Erdös et Straus. Ce résultat est une conséquence de l'identité suivante, évidente à vérifier :

$$\frac{4}{n} = \frac{1}{m\,n} + \frac{4m-1}{m\,n+d} + \frac{(4m-1)d}{(m\,n+d)n\,m}. \tag{1}$$

1 Quelques résultats partiels classiques

1. Si n vérifie la conjecture alors $k\,n$ également, car si : $\dfrac{4}{n} = \dfrac{1}{x} + \dfrac{1}{y} + \dfrac{1}{z}$
   alors : $\dfrac{4}{k\,n} = \dfrac{1}{k\,x} + \dfrac{1}{k\,y} + \dfrac{1}{k\,z}$.
   Ainsi tout multiple d'un nombre premier vérifiant la conjecture la vérifie aussi.
   Conséquence : comme $\dfrac{4}{2} = 2 = 1 + \dfrac{1}{2} + \dfrac{1}{2}$ alors $\dfrac{4}{2\,n} = \dfrac{1}{n} + \dfrac{1}{2\,n} + \dfrac{1}{2\,n}$.
   Autrement dit, tout nombre pair vérifie la conjecture.
   De même tout multiple de 3 vérifie la conjecture car $\dfrac{4}{3} = 1 + \dfrac{1}{4} + \dfrac{1}{12} = 1 + \dfrac{1}{6} + \dfrac{1}{6}$,
   ou tout multiple de 5 $\left(\dfrac{4}{5} = \dfrac{1}{5} + \dfrac{1}{2} + \dfrac{1}{10}\right)$ ou tout multiple de 7 $\left(\dfrac{4}{7} = \dfrac{1}{21} + \dfrac{1}{2} + \dfrac{1}{42}\right)$, etc.
   Mais comment trouver une décomposition générique pour tout nombre premier ?

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

On remarquera que cette identité est un cas particulier de l'identité (1), en posant $n = 2 + 3x$, $m = 1$ et $d = 1$.

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 :
   soit p un nombre premier, si p modulo 24 est différent de 1 et de 17, alors cette méthode marche. En effet en posant $p = 24k + b$, z s'exprime comme un polynôme de degré 4 en k à coefficients entiers si b est différent de 1 et de 17.

4. Encore une autre approche, c'est celle qui consiste à écrire $\frac{4}{p}$ 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 $\frac{4}{p} = \frac{1}{x} + \frac{1}{y}$ et qui montre bien les difficultés pour résoudre la conjecture d'Erdös-Straus.

   Soit n un entier égal à 3 modulo 4, i.e. $n = 4k - 1$ alors $\frac{4}{n}$ s'écrit comme somme de deux fractions égyptiennes : $\frac{4}{n} = \frac{1}{k\,n} + \frac{1}{k}$, puis de trois, en utilisant l'identité $\frac{1}{k} = \frac{1}{k+1} + \frac{1}{k(k+1)}$: $\frac{4}{n} = \frac{1}{(k+1)\,n} + \frac{1}{k} + \frac{1}{k(k+1)\,n}$. Il est facile de voir qu'en posant $m = k + 1 = \frac{n+5}{4}$ et $d = 1$, cette décomposition découle directement de l'identité (1).

5. Il est bien connu que tout nombre n égal à 2 ou à 3 modulo 5 vérifie la conjecture d'Erdös-Straus ; en voici une preuve élémentaire à partir de l'identité (1) :
   Si $n = 2$ modulo 5, on pose $m = 4$ et $d = 2$ et si $n = 3$ modulo 5, on pose $m = 4$ et $d = 8$; l'identité de départ résoud la conjecture.

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 Un résultat intermédiaire

Avant d'établir l'identité (1), nous avons utilisé un certain nombre de formules (et d'algorithmes associés), l'idée sous-jacente à ces formules étant d'éviter le plus possible le recours à la fonction *partie entière*. Voici le principal résultat intermédiaire qui, outre le fait qu'il nous a conduit à l'identité présentée, possède un intérêt en lui-même.

Lemme 1 sur les restes modulo $4m-1$: 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 $x = mp$,
$y = E\left(\frac{p}{4}\right) + 1 = mk + 1 + E\left(\frac{mb}{4m-1}\right)$ 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 $b > 0$ tels que z soit un polynôme en k à coefficients entiers, alors $4m-2$ et $4m-5$ appartiennent à $T(m)$ (pour $m > 1$). Par exemple $T(1) = \{2\}$, $T(2) = \{3, 5, 6\}$, $T(3) = \{7, 8, 10\}$, $T(4) = \{3, 5, 6, 7, 10, 11, 12, 13, 14\}$, $T(5) = \{15, 18\}$, etc. .
La preuve est élémentaire pour i), et un algorithme simple permet de calculer l'ensemble des restes possibles $T(m)$.

Remarques :

- 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. Ceci se montre immédiatement en utilisant ce lemme avec $m = 1$, 2 et 4, et l'utilisation du théorème des restes chinois. 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 $T(m)$, pour $m > 4$.
- Ce lemme conduit à une infinité de formules. pour $p = (4m-1)k + 4m - 2$, $x = mp$, $y = m(k+1)$ et $z = yp$; pour $p = (4m-1)k + 4m - 5$, $x = mp$, $y = m(k+1) - 1$ et $z = yp$; pour m pair, $4m-3$, $4m-9$ puis $4m-17$ (pour m pas trop petit), etc. sont dans $T(m)$. Ceci donne par exemple :
  pour $p = (4m-1)k + 4m - 3$, $x = mp$, $y = m(p+2)/(4m-1)$ et $z = yp/2$;
  pour $p = (4m-1)k + 4m - 9$, $x = mp$, $y = (mp+2)/(4m-1)$ et $z = myp/2$.
- Mutatis mutandis, on obtient le même type de lemme pour 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 $\frac{a}{b}$. Les algorithmes mis en œuvre sont très rapides ; par exemple, pour les 100000 premiers nombres premiers $p > 5$, **toutes** les fractions $\frac{5}{p}$ sont décomposées en somme de trois fractions égyptiennes, le total en quelques secondes sur un portable avec un logiciel de calcul formel.

– Il faut remarquer enfin que si l'on supprime le recours au calcul d'une partie entière, il en reste encore une et dans le programme principal et dans le calcul des ensembles $T(m)$ de restes possibles. Cependant, il est apparu une propriété intéressante, celle de constater que dans la décomposition $\frac{4}{p} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$, basée sur ce lemme, pour tout nombre premier $p < 10^8$, z est un multiple de p, (comme x). C'est l'étude de cette propriété qui nous a permis de passer des ensembles $T(m)$ de restes possibles à ceux de diviseurs de m^2, et ainsi d'aboutir au résultat (1) et surtout de se passer de tout recours à la fonction *partie entière*.

3 Sur la conjecture d'Erdös-Straus

Le lemme précédent conduit à la conjecture suivante qui, si elle est démontrée, prouve la conjecture d'Erdös-Straus.

Conjecture 1 : pour tout nombre premier p il existe un entier m tel que p modulo $(4m-1)$ soit dans $T(m)$ (défini dans le lemme).

Lemme 2 l'identité de base : soient a et b deux entiers, alors pour tout couple d'entiers m et d on a :

$$\frac{a}{b} = \frac{1}{m\,b} + \frac{a\,m-1}{m\,b+d} + \frac{(a\,m-1)d}{(m\,b+d)b\,m}. \qquad (2)$$

Cette identité n'est qu'une généralisation immédiate de la formule (1) et conduit au

Corollaire : soit a un entier p un nombre premier ; soit m un entier et d un diviseur de m^2, si $m\,p+d$ est divisible par $a\,m-1$ alors l'identité (2) donne une décomposition de $\frac{a}{p}$ en somme de trois fractions égyptiennes.

La preuve, très simple, ne pose pas de problème ; on peut préciser que pour a=4, la condition $m\,p+d$ est divisible par $a\,m-1$ est équivalente à la condition $p+4d$ est divisible par $4\,m-1$. D'où, par exemple pour a=4, la

Conjecture 2 : pour tout nombre premier p il existe un entier m et un diviseur d de m^2 tels que $m\,p+d$ soit divisible par $4m-1$.

Cette conjecture 2 est vérifiée en quelques minutes (d'ordinateur) pour tout nombre premier $p < 10^9$; sa véracité entraine évidemment celle de la conjecture d'Erdös-Straus.

Signalons que pour $p < 10^9$, on trouve un entier m majoré par 1000 (exactement 816). Voici un programme de base très efficace (avec le logiciel maple) qui à p associe d'une part la décomposition de $\frac{4}{p}$ en somme de trois fractions égyptiennes et d'autre part les paramètres m et d utilisés.

```
> w:=time():with(numtheory):
> Dm:=[seq(divisors(m^2),m=1..1000)]:
> Erdos3octe:=proc(p)
> local x,y,z,d,c,m;
> global Dm;
> for m from 1 to 1000 do
> for d in Dm[m] do
> if p+4*d mod (4*m-1)=0 then c:=(m*p+d)/(4*m-1):
> return([p,[m*p,c,c*m*p/d],[m,d]]):
> fi:od:
> od:
> return([p,echec]);
> end:
> P:=[seq(ithprime(u),u=1..100000)]:
> test:=map(u->Erdos3octe(u),P):nops(test);time()-w;
                                100000
                                10.112

> #les vérifications
> select(u->nops(u)=2 ,test);#pas d'échec
                                  []

>convert(map(u->4/op(1,u)-1/op(1,op(2,u))-1/op(2,op(2,u))-1/op(3,op(2,u)),
test),set);#décomposition en somme de trois fractions égyptiennes exacte.
                                 {0}

> convert(map(u->is(op(2,op(2,u)),integer),test),set);#les y sont entiers
                                {true}

> convert(map(u->is(op(3,op(2,u)),integer),test),set);#les z sont entiers
                                {true}

> convert(map(u->op(1,op(3,u)),test),set);#les valeurs prises par m
  {1, 2, 3, 4, 5, 6, 8, 10, 11, 12, 14, 15, 17, 18, 20, 21, 22, 24,
        25, 26, 27, 28, 30, 32, 33, 35, 36, 38, 39, 40, 41, 42, 45,
        46, 48, 50, 51, 52, 54, 55, 56, 57, 60, 63, 65, 66, 70, 72,
        75, 76, 78, 81, 84, 85, 90, 96, 98, 102, 105, 120, 130, 147,
```

```
        174}

> Erdos3octe(3361);#un exemple clef
                [3361, [84025, 850, 571370], [25, 125]]
```

En une dizaine de secondes, les 100 000 premiers nombres premiers sont traités.

Sur un résultat de Mordell :
Dans son livre, il établit que $\frac{4}{n}$ admet une décomposition de la forme : $\frac{4}{n}=\frac{1}{x}+\frac{1}{y\,n}+\frac{1}{z\,n}$, si et seulement si il existe quatre entiers A, B, C et D, tels que A, B et C soient premiers entre eux deux à deux et $x = BCD$, $y = ABD$ et $z = ACD$, i.e. on a :

$$\frac{4}{n}=\frac{1}{BCD}+\frac{1}{ABD\,n}+\frac{1}{ACD\,n}. \tag{3}$$

Montrons que (3) se met sous la forme (1). Pour cela, posons $m = ABD$ et $d = B^2D$ qui divise m^2. L'équation (3) devient, en exprimant A et D en fonction de m, d, B et C :

$$\frac{4}{n}=\frac{B}{C\,d}+\frac{1}{m\,n}+\frac{B}{C\,m\,n}, \tag{4}$$

et donc :

$$\frac{4}{n}-\frac{1}{m\,n}=\frac{4m-1}{m\,n}=\frac{B}{C\,d}\frac{m\,n+d}{m\,n}, \tag{5}$$

qui se réduit à :

$$\frac{C\,d}{B}=\frac{m\,n+d}{4m-1}. \tag{6}$$

Or B divise $d = B^2D$, donc $\frac{m\,n+d}{4m-1}$ est un entier, cqfd.

C'est en choisissant certaines valeurs pour A, B, C et D que Mordell obtient le résultat classique : 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.
Puis en 1999, Allan Swett vérifie que la conjecture est vraie pour $p < 10^{14}$ à l'aide d'un algorithme s'inspirant du résultat de Mordell et ayant des similitudes avec l'algorithme utilisant le lemme 1 ci-dessus. L'avantage incontestable de la formule (1) est de n'utiliser que deux paramètres m et d, au lieu des quatre paramètres A, B, C et D.
En effet il suffit de considérer les valeurs 1,2 et 4 de m pour retrouver le résultat classique et le prolonger ; par exemple, avec $m = 3$, il ne reste que 36 classes modulo 9240 qui échappent à la conjecture, etc.

Remarque : il existe plusieurs algorithmes possibles utilisant la formule (1) ne donnant pas forcément la même décomposition. En voici un autre, plus élémentaire car n'utilisant pas la connaissance a priori des diviseurs de m, qui est plus lent pour les petits premiers, mais plus rapide pour les grands premiers (au moins deux fois plus véloce pour $p > 10^{14}$).

```
> Erdos3octebis:=proc(p)
> local x,y,z,d,c,m,mm;
> if p mod 3=2 then return([p,[p,(p+1)/3,(p+1)/3*p],[1,1]]):fi:#m=d=1
> for m from 2 to 1500 do mm:=4*m-1:
> d:=mm-(m*p mod mm);
> if m^2 mod d=0 and m*(m*p+d) mod (d*mm)=0 then c:=(m*p+d)/mm:
> return([p,[m*p,c,c*m*p/d],[m,d]]):
> fi:
> od:
> return([p,echec]);
> end:
> Erdos3octebis(3361);Erdos3octe(3361);
              [3361, [974690, 841, 28266010], [290, 29]]
               [3361, [84025, 850, 571370], [25, 125]]
```

Mais en l'an 2000 A. Schinzel prouve un résultat négatif dont un cas particulier peut s'énoncer ainsi : il n'existe pas de formule polynomiale en n telle que $\frac{4}{n} = \frac{1}{x} + \frac{1}{y\,n} + \frac{1}{z\,n}$.
Ce résultat signifie en particulier qu'on ne peut espérer démontrer la conjecture d'Erdös-Straus en utilisant uniquement la formule (1) (ou la formule équivalente (3) de Mordell) ; il faut d'autres formules.

En voici une, par exemple, utilisable pour p entier égal à 1 modulo 4 :

$$\frac{4}{p} = \frac{4}{p+4\,a-1} + \frac{4(4\,a-1)}{(4\,d+p+4\,a-1)p} + \frac{16\,d(4\,a-1)}{(p+4\,a-1)(4\,d+p+4\,a-1)p} \tag{7}$$

qui part d'un x petit $\left(\frac{p-1}{4} + a,\ a > 0\right)$, qui définit d tel que $\frac{d+x}{4*a-1}$ soit un entier que l'on nomme m (ces entiers d et m existent toujours) ; il suffit alors de vérifier que d divise m^2 pour obtenir une décomposition.
Cette identité ne tombe pas du ciel puisque je viens de décrire le processus algorithmique de son établissement. Les décompositions obtenues sont évidemment très différentes de celles obtenues par la formule (1), d'une part parce que l'on prend x le plus petit possible et d'autre part parce que z est un polynôme *a priori* de degré 3 en p, au lieu de degré 2 par la formule (1). Cette formule décompose les carrés des nombres premiers > 2 (égaux à 1 modulo 4), ce que ne permet pas la formule (1).
Ces deux identités (1) et (7) suffisent-elles pour résoudre théoriquement la conjecture, ou faut-il en établir d'autres ?

Bibliographie

Guy R. Unsolved Problems in Number Theory, 3ème édition, Springer, 2003, problème D11, pp 252-262.
Mordell L.J. Diophantine equations, London, New York : Academic press, 1969, chapter 30.
Schinzel A. On sums of three unit fractions with polynomial denominators. Funct. Approx. Comment. Math. 28 : 187-194, 2000.
page Internet d'Allan Swett : http ://math.uindy.edu/swett/esc.htm.
page Internet Sloane : http ://www.research.att.com/ njas/sequences/A073101.

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, Août 2009.