Sur la conjecture d'Erdös-Straus

Michel Mizony, ICJ, université Lyon1, Octobre 2009

Le problème ▸ Voir

Une formule ▸ Voir

Des programmes ▸ Voir

Le problème

L'énoncé ci-dessous est la conjecture d'Erdös et Straus. Plusieurs généralisations et problèmes ont été proposées depuis. La question de fond étant :
« Quels rapports peut-on établir entre décompositions de fractions en somme de trois fractions égyptiennes et connaissance des nombres premiers ? »

Toute fraction $\frac{4}{n}$ peut-elle s'écrire sous la forme :
$$\frac{1}{x}+\frac{1}{y}+\frac{1}{z}\ \textbf{?}$$

Existe-t-il une formule donnant une décomposition :
$$\frac{4}{n}=\frac{1}{x}+\frac{1}{y}+\frac{1}{z}\ ?$$

Et pour deux entiers naturels a et b, sous quelles conditions a-t-on :
$$\frac{a}{b}=\frac{1}{x}+\frac{1}{y}+\frac{1}{z}\ ?$$

Le problème

1948, énoncé de la conjecture par Erdös et Straus.
1969, les résultats de Mordell.
1999, vérification de la conjecture pour $n < 10^{14}$ par Swett.
2000, le résultat négatif de Schinzel : pas de solution générale par une formule polynomiale.

Evidences : si n vérifie la conjecture, kn également. Si n est premier et $\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$, alors 1 ou 2 des trois nombres x, y et z sont divisibles par p.
Il existe une formule polynomiale pour n=2 modulo 3, une autre pour n=3 modulo 4, etc..
Il reste à démontrer la conjecture pour n premier et égal à 1 modulo 24.

Un résultat de **Mordell** :
si $\frac{4}{n} = \frac{1}{x} + \frac{1}{yn} + \frac{1}{zn}$, alors il existe 4 entiers A, B, C et D, avec A, B, C premiers entre eux deux à deux tels que x=BCD, y=ABD et z=ACD.
En conséquence, il reste à démontrer la conjecture pour n premier et égal à 1, 121, 169, 289, 361 et 529 modulo 840.

Une formule

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

Sans approfondir ici, il est clair que cette identité n'est pas tombée du ciel, mais est le fruit d'une grande quantité d'algorithmes mis en œuvre ayant deux buts :
1- être efficace : passer de 100 décompositions à la seconde à 20000 n'est pas anodin.
2- être le plus proche possible d'une preuve avec papier et crayon, l'idée sous-jacente à ces algorithmes et formules ayant été d'éviter le plus possible le recours à la fonction *partie entière*.
Il n'en reste pas moins vrai que je suis incapable de dire pourquoi je l'ai écrite ce 13 Août 2009, et généralisée, ce qui m'était évident, dans l'heure qui suit :
Soient a et b deux entiers, alors pour tout couple d'entiers m et d on a l'identité :

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

Sur la formule (1)

Proposition : Cette formule (1) est équivalente à celle de Mordell.

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

Pour cela, en suivant une remarque de L. Habsieger, posons $m = ABD$ et $d = B^2 D$ qui divise m^2 dans cette équation. Exprimons A et D en fonction de m, d, B et C :

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

qui se réduit à

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

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

Sur la formule (1)

L'intérêt principal de cette formule (1) qu'il faut lire sous la forme :

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

est d'obtenir une décomposition de $\frac{4}{n}$ en somme de trois fractions égyptiennes sous la seule condition que $m\,n + d$ soit divisible par $4m-1$. D'où des algorithmes efficaces.
Un deuxième intérêt est de reformuler la conjecture d'Erdös-Straus sous la forme :

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 $4m-1$.
La validité de cette conjecture (vérifiée en quelques minutes pour $p < 10^9$) entraîne celle d'Erdös-Straus.

Sur la formule (1), suite

Cette formulation établit de plus un lien étroit entre décompositions en somme de fractions égyptiennes et une propriété des nombres premiers. A ma connaissance, je n'ai rien remarqué dans la littérature, à propos de cette conjecture ; cependant un rapport existe avec les nombres pentagonaux, cf. Sloane A144065 par exemple.

Retour sur le résultat de Schinzel : cette formule (1) donne naissance à une formule polynômiale pour chaque m et pour chaque d diviseur de m^2, autrement dit à une infinité de formules polynômiales, ainsi, sans contredire ce résultat, on peut espérer prouver la conjecture. On peut exprimer les choses autrement en disant que cette infinité inévitable de formules donne une heuristique à ce résultat de Schinzel.

Sur la formule (1), les nombres pentagonaux

En considérant $m \in \{1, 2, 4\}$ la formule (1) permet de retrouver le résultat théorique donnant les 6 classes modulo 840 pour lesquelles la conjecture d'Erdös-Straus n'est pas démontrée ; s'il l'on considère $m \in \{1, 2, 3, 4, 14\}$, alors il ne reste plus que 36 classes modulo $9240 = 11 \times 840$, ce qui améliore beaucoup le résultat précédent (il faut comprendre 14 à travers le fait que $14 * 4 - 1$ est multiple de 11) ; etc. mais cette piste s'avère vaine.
Par contre 24 est le plus grand nombre pour lequel il n'existe plus qu'une seule classe à étudier. Soit donc les nombres de la forme $n = 24k + 1$ et considérons les nombres k pour lesquels il existe m et d (divisant m^2) donnant une décomposition de $\frac{4}{n}$, via cette formule (1). L'expérimentation sur ordinateur montre que ce sont les nombres non pentagonaux, autrement dit les nombres k tels que n ne soit pas un carré. Une piste sérieuse qui conduit à la conjecture :

Conjecture 3 : Pour tout nombre k non pentagonal alors pour $n = 24k + 1$, il existe m et d divisant m^2 tels que $\dfrac{m\,n + d}{4m - 1}$ soit un entier.
La validité de cette conjecture entraîne celle d'Erdös-Straus.

On généralise la formule (1)

Pour n admettant un facteur r, en particulier pour n=24k+1 où k est un nombre pentagonal, il est pratique d'utiliser l'identité suivante qui généralise, pour r=1, l'identité de base :

$$\frac{4}{n} = \frac{1}{m\,n} + \frac{4m-1}{(m\frac{n}{r}+d)r} + \frac{(4m-1)d}{(m\frac{n}{r}+d)m\,n}. \tag{5}$$

Evidemment cette formule donne une décomposition si r divise n, 4m-1 divise $m\frac{n}{r}+d$ et d divise m^2 et donne lieu à un algorithme récursif qui décompose toute fraction $\frac{4}{n}$.

Des programmes

Le principe algorithmique est basé sur les identités (1) et (5) ; il nécessite une initialisation qui construit l'ensemble des diviseurs d de m^2. Nous donnons un programme général, écrit en "maple 9" qui fournit la décomposition des fractions $\frac{4}{n}$ en somme de trois fractions égyptiennes. On peut en déduire un algorithme encore plus rapide qui décompose les nombres de la forme $n = 24k + 1$. Ces algorithmes sont l'aboutissement d'une dizaine d'autres, toujours de plus en plus concis, théoriques et efficaces (et qui m'ont permis de mettre en évidence les identités).

Un programme de décomposition

```
> with(numtheory) :Dm :=[seq(divisors(m^2),m=1..3500)] :
> ErdosStraus :=proc(p)
local m, d, c ; global Dm ;
    for m to 3500 do #début du corps du programme
        if 1 < m and p mod m = 0 then
            return([p, m, ErdosStraus(p/m)]) end if ;# récursivité
        for d in Dm[m] do
            if (m*p + 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]]) end if
        end do ;
    end do ;#fin du corps du programme
    m :=sqrt(p) ;# pour les nombres pentagonaux restants
    if is(m, integer) then return([p, m, ErdosStraus(m)]) end if ;
    return(p = echec)
end proc :
ErdosStraus(3361) ; [3361, [84025, 850, 571370], [25, 125]]
ErdosStraus(2031121) ;
[2031121, [1267419504, 507984, 1117758384236], [624, 576]]
```

Pour les entiers de la forme 24k+1

Soit p un nombre de la forme 24k+1 et m et d (diviseur de m^2) ; dire que mp+d =0 modulo (4m-1) équivaut à dire que k appartient à un certain ensemble que l'on notera R[m] dans $Z/(4m-1)Z$. Voici une procédure permettant de construire facilement ces ensembles R[m]. La conjecture d'Erdös-Straus est vraie si les ensembles $K[m] = \{k/\ k\ modulo\ (4m-1) \in R[m]\}$ recouvrent le complémentaire des nombres pentagonaux.

```
> construitRm24 :=proc(m)
local v,d ;global Dm ;
map(v->op(2,op(v)),{seq(msolve((24*k+1)*m+d=0,4*m-1),d=Dm[m])}) ;
end :
> R :=[seq(construitRm24(m),m=1..1000)] :
> R[1..6] ;
[{}, {3, 4, 6}, {3, 9, 10}, {3, 4, 8, 9, 13, 14}, {11, 14, 18}, {6, 9, 10, 14, 16, 18, 19, 20, 21}]
```

A partir de là on construit un algorithme encore plus efficace pour donner une décomposition en somme en trois fractions égyptiennes de la fraction $\frac{4}{24k+1}$.

En particulier pour tout premier inférieur à 10^{11}, on obtient un m inférieur à 1000. Mais $m = 2295$ pour

ErdosStraus(240000095140208881) ;

[240000095140208881, [550800218346779381895, 60006560447410326, 72007901082075867184856155781526030], [2295, 459]]

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/A144065.

Conclusion

C'est en recherchant des algorithmes de plus en plus efficaces et en cherchant à se passer de la fonction partie entière que petit à petit a émergé l'identité. Mais celle-ci ne semble pas permettre de pouvoir montrer facilement l'existence et donc la conjecture. Par ailleurs, à l'instar des babyloniens, j'ai plus été intéressé par la construction d'algorithmes que par l'élaboration de preuves.

Retour

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 $z = \frac{1}{\frac{p}{4} - \frac{1}{x} - \frac{1}{y}}$; alors : $x = 6k + 1 + E(\frac{b}{4})$, i.e. un polynôme en k, les 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. Pour quelles valeurs de b ces polynômes sont-ils à coefficients entiers ?

Lemme 1 : Soit $p = 24k + b$; pour b différent de 1 et 17, z est un polynôme en k à coefficients entiers. Pour $b = 1$, 5, 7, 11, 13, 17, 19 et 23, ces polynômes sont :

- 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.

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 $x=mp$,
$y=E\left(p/4\right)+1=mk+1+E\left(\frac{mb}{4m-1}\right)$ et

$$z=\frac{pym}{(4m-1)\times\left(1+E\left(\frac{mb}{4m-1}\right)-mb\right)};$$ 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) est élémentaire ; cependant nous allons donner les polynômes obtenus pour montrer ii), car ce point entraîne une conséquence importante sur l'existence d'une décomposition.

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

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 ou 17 modulo 24 ;
D'après le lemme 2, en utilisant T(1), on règle le cas des nombres égaux à 17 modulo 24. L'utilisation de T(2) puis de T(4) et du lemme chinois nous dit qu'il reste à étudier les nombres égaux à 1, 121, 169, 289, 361 et 529 modulo 840. 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 : Soit b un reste de p modulo 4*m-1 alors il existe un diviseur d de m^2 défini par la formule : $b * d \; = \; 3 * m - 1$ modulo $4 * m - 1$; en posant $x = m\,p$, $y = \frac{m}{d}\,\frac{d\,p+m}{4m-1}$ et $z = \frac{y\,d}{m}p$, on a $\frac{4}{p} - \frac{1}{x} - \frac{1}{y} - \frac{1}{z} = 0$ et, pour que z soit entier, il faut que $d\,p + m$ soit divisible par $4m - 1$.

D'où un nouvel algorithme, très simple et efficace, sans calcul de partie entière.

Une autre identité

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

$$\frac{4}{p} = \frac{4}{p+4\,a-1} + \frac{4(4\,a-1)}{(4\,d+p+4\,a-1)p} + \frac{16\,d(4\,a-1)}{(p+4\,a-1)(4\,d+p+4\,a-1)p}, \quad (6)$$

qui part d'un x petit ($\frac{p-1}{4} + a$, $a > 0$), 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 (6) suffiront-elles pour résoudre théoriquement la conjecture, ou faut-il en établir d'autres ?

Expérience :

Expérimenter avec maple