15 janvier 2009

Cours de Théorie des Nombres MM020

L'équation dite de Pell–Fermat

$x^2 - dy^2 = \pm 1$

Michel Waldschmidt

Institut de Mathématiques de Jussieu & CIMPA

http ://www.math.jussieu.fr/∼miw/

L'équation dite de Pell–Fermat

L'équation $x^2 - dy^2 = \pm 1$, où les inconnues x et y sont des entiers positifs tandis que d est un entier positif fixé qui n'est pas un carré, a été baptisée par erreur du nom de Pell par Euler. Elle a fait l'objet de recherches par l'école mathématique indienne, depuis Brahmagupta (628) qui a résolu le cas $d = 92$, puis Bhaskara II (1150) pour $d = 61$ et Narayana (au 14-ième siècle) pour $d = 103$. Quand on apprend que les plus petites solutions pour ces valeurs de d sont respectivement

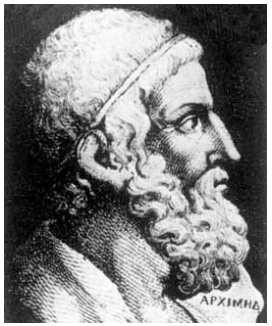
$$1\,151^2 - 92 \cdot 120^2 = 1, \qquad 29\,718^2 - 61 \cdot 3\,805^2 = -1$$

et

$$227\,528^2 - 103 \cdot 22\,419^2 = 1,$$

on comprend que ces solutions n'ont pas été trouvées par hasard ni même au moyen d'une recherche exhaustive.
Après une brève présentation de cette longue histoire nous expliquerons le lien avec l'approximation diophantienne et les fractions continues, puis nous indiquerons quelques développements plus récents du sujet.

Problème des bovins d'Archimède



Le dieu soleil Hélios possédait un immense troupeau de bovins (boeufs). C'était un troupeau de taureaux et de vaches, dont une première partie était blanche, une deuxième partie était noire, une troisième partie était tachetée, et la quatrième partie était brune.

Problème des boeufs

Parmi les taureaux, le nombre de ceux qui étaient blancs dépassait le nombre des taureaux bruns de la moitié plus un tiers du nombre des taureaux noirs.
Le nombre des taureaux noirs dépassait le nombre des taureaux bruns d'un quart plus un cinquième du nombre des taureaux tachetés.
Enfin le nombre des taureaux tachetés dépassait celui des bruns d'un sixième plus un septième du nombre des taureaux blancs.

Premier système d'équations

$B =$ taureaux blancs, $N =$ taureaux noirs,
$T =$ taureaux bruns, $X =$ taureaux tachetés

$$B - \left(\frac{1}{2} + \frac{1}{3}\right) N = N - \left(\frac{1}{4} + \frac{1}{5}\right) X$$
$$= X - \left(\frac{1}{6} + \frac{1}{7}\right) B = T.$$

À un facteur près, la solution est

$$B_0 = 2226,\ N_0 = 1602,\ X_0 = 1580,\ T_0 = 891.$$

Problème des boeufs

Parmi les vaches, le nombre des blanches était égal au tiers augmenté du quart du nombre total des bovins noirs.
Le nombre des vaches noires était égal au quart augmenté du cinquième du nombre total des bovins tachetés.
Le nombre des vaches tachetées était égal au cinquième augmenté du sixième du nombre total des bovins bruns.
Enfin le nombre des vaches brunes était égal au sixième plus un septième du nombre total des bovins blancs.

Deuxième système d'équations

$b =$ vaches blanches, $n =$ vaches noires,
$t =$ vaches brunes, $x =$ vaches tachetées

$$b = \left(\frac{1}{3} + \frac{1}{4}\right)(N + n), \quad n = \left(\frac{1}{4} + \frac{1}{5}\right)(X + x),$$
$$t = \left(\frac{1}{6} + \frac{1}{7}\right)(B + b), \quad x = \left(\frac{1}{5} + \frac{1}{6}\right)(T + t).$$

Puisque les solutions b, n, x, t recherchées doivent être entières, on montre que

$$(B, N, X, T) = k \times 4657 \times (B_0, N_0, X_0, T_0).$$

Problème des boeufs

Ami, si tu peux me dire exactement combien il y avait de boeufs d'Hélios en précisant le nombre des taureaux robustes et, à part, celui des vaches pour chaque couleur, tu ne seras, certes, pas appelé ignorant ni inculte en matière de nombres, mais tu ne te feras pas pour autant ranger parmi les savants.

Problème des boeufs

Mais examine encore toutes les manières dont les boeufs d'Hélios ont été groupés.

En réunissant les taureaux blancs et les noirs, on pouvait les ranger en un carré parfait.

Les bruns et les tachetés, réunis, se rangeaient de leur côté de façon à former une figure triangulaire parfaite.

Contraintes arithmétiques

$$\begin{aligned} B+N &= \text{un carré,} \\ T+X &= \text{un nombre triangulaire.} \end{aligned}$$

Comme fonction de l'entier k, on a $B+N=4Ak$ avec $A=3\cdot 11\cdot 29\cdot 4657$ sans facteurs carrés. On a donc $k=AU^2$ avec U entier. D'un autre côté si $T+X$ est un nombre triangulaire $(=m(m+1)/2)$, alors $8(T+X)+1$ est un carré $(2m+1)^2=V^2$. En écrivant $T+X=Wk$ avec $W=7\cdot 353\cdot 4657$, on obtient

$$V^2-DU^2=1$$

avec $D=8AW=(2\cdot 4657)^2\cdot 2\cdot 3\cdot 7\cdot 11\cdot 29\cdot 353$.

$$2\cdot 3\cdot 7\cdot 11\cdot 29\cdot 353=4\,729\,494.$$

$$D=(2\cdot 4657)^2\cdot 4\,729\,494=410\,286\,423\,278\,424.$$

Problème des boeufs

Quand tu auras trouvé, ami, et embrassé dans ton esprit la solution de toutes ces questions, en indiquant toutes les mesures de ces multitudes, rentre chez toi, te glorifiant de ta victoire, et sache qu'on te juge arrivé à la perfection dans cette science.

Histoire

Archimèdes : 287–212 AC – lettre à Eratosthènes de Cyrène
Odyssée d'Homère - les boeufs du Soleil

Gotthold Ephraim Lessing : 1729–1781 – Bibliothèque Herzog August, Wolfenbüttel, 1773

C.F. Meyer, 1867

A. Amthor, 1880 : le nombre de chiffres de la plus petite solution est $206\,545$, et celle-ci commence par 776.
B. Krumbiegel et A. Amthor, Das Problema Bovinum des Archimedes, Historisch-literarische Abteilung der Zeitschrift für Mathematik und Physik, **25** *(1880), 121–136, 153–171.*

Histoire (suite)

A.H. Bell, The "Cattle Problem" by Archimedies 251 BC, Amer. Math. Monthly **2** (1895), 140–141.
Calcul des 31 premiers et 12 derniers chiffres décimaux.

"Since it has been calculated that it would take the work of a thousand men for a thousand years to determine the complete number [of cattle], it is obvious that the world will never have a complete solution"
Pre-computer-age thinking from a letter to The New York Times, January 18, 1931

Histoire (suite)

H.C. Williams, R.A. German and C.R. Zarnke, Solution of the cattle problem of Archimedes, Math. of Computation **19** (1965), 671–674.

H.G. Nelson, A solution to Archimedes' cattle problem, J. Recreational Math. **13** (3) (1980–81), 162–176.

I. Vardi, Archimedes' Cattle Problem, Amer. Math. Monthly **105** (1998), 305-319.

H.W. Lenstra Jr, Solving the Pell Equation, Notices of the A.M.S. **49** (2) (2002) 182–192.

La solution du problème d'Archimède

Équation $x^2 - 410\,286\,423\,278\,424 y^2 = 1$.

Sortie imprimante de la plus petite solution avec $206\,545$ chiffres décimaux : 47 pages (H.G. Nelson, 1980).

$$77602714\ldots\ldots237983357\ldots\ldots55081800$$

où chacun des $\ldots\ldots$ représente 34420 chiffres.

Grands nombres

Un nombre écrit à l'aide de 3 chiffres mais ayant près de 370 millions de chiffres décimaux :

Le nombre de chiffres décimaux de 9^{9^9} *est*

$$\left[9^9 \frac{\log 9}{\log 10}\right] = 369\,693\,100.$$

$10^{10^{10}}$ a $1 + 10^{10}$ chiffres décimaux (10 milliards).

Ilan Vardi

Archimedes' Cattle Problem, American Math. Monthly **105** (1998), 305-319.

$$\left[\frac{25194541}{184119152}\,(10993198673282973497986623282143354390108804 9+ 50549485234315033074477819735540408986340\sqrt{4729494})^{4658}\right]$$

Antti Nygrén, "A simple solution to Archimedes' cattle problem", University of Oulu Linnanmaa, Oulu, Finland Acta Universitatis Ouluensis Scientiae Rerum Naturalium, 2001.
50 premiers chiffres
77602714064868182695302328332138866642323224059233
50 derniers chiffres :
05994630144292500354883118973723406626719455081800

Résolution de l'équation de Pell

H.W. Lenstra Jr,
Solving the Pell Equation,
Notices of the A.M.S.
49 (2) (2002) 182–192.

Solution du problème d'Archimède

All solutions to the cattle problem of Archimedes

$$w = 300\,426607\,914281\,713365 \cdot \sqrt{609} + 84\,129507\,677858\,393258 \cdot \sqrt{7766}$$

$$k_j = (w^{4658 \cdot j} - w^{-4658 \cdot j})^2 / 368\,238304 \qquad (j = 1,\ 2,\ 3,\ \ldots)$$

jth solution	*bulls*	*cows*	*all cattle*
white	$10\,366482 \cdot k_j$	$7\,206360 \cdot k_j$	$17\,572842 \cdot k_j$
black	$7\,460514 \cdot k_j$	$4\,893246 \cdot k_j$	$12\,353760 \cdot k_j$
dappled	$7\,358060 \cdot k_j$	$3\,515820 \cdot k_j$	$10\,873880 \cdot k_j$
brown	$4\,149387 \cdot k_j$	$5\,439213 \cdot k_j$	$9\,588600 \cdot k_j$
all colors	$29\,334443 \cdot k_j$	$21\,054639 \cdot k_j$	$50\,389082 \cdot k_j$

Figure 4.

H.W. Lenstra Jr,
Solving the Pell Equation,
Notices of the A.M.S.
49 (2) (2002) 182–192.

Problème de Brahmagupta (628)

Brahmasphutasiddhanta : Résoudre en entiers l'équation

$$x^2 - 92y^2 = 1$$

La plus petite solution est

$$x = 1151, \qquad y = 120.$$

Méthode de composition : *samasa*.

http ://mathworld.wolfram.com/BrahmaguptasProblem.html

Bhaskara II (12-ième siècle)

Lilavati Ujjain (Inde)

(*Bijaganita*, 1150)

$$x^2 - 61y^2 = 1$$

$$x = 1\,766\,319\,049, \qquad y = 226\,153\,980.$$

Méthode cyclique (Chakravala) de Brahmagupta.

Narayana (14-ième siècle)

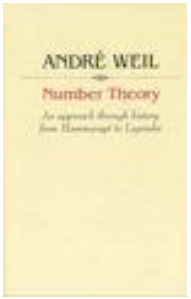
Narayana cows (*Tom Johnson*)

$$x^2 - 103y^2 = 1$$

$$x = 227\,528, \qquad y = 22\,419.$$

Référence aux travaux des mathématiciens indiens

André Weil
Number theory. :
An approach through history. From Hammurapi to Legendre.
Birkhäuser Boston, Inc., Boston, Mass., (1984) 375 pp.
MR 85c :01004



Histoire

John Pell : 1610–1685

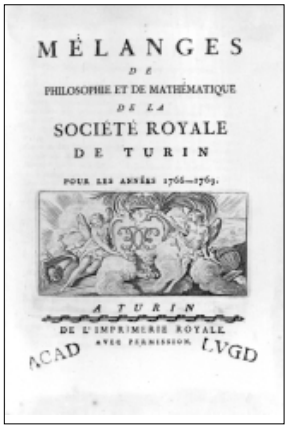
Pierre de Fermat : 1601–1665
Lettre à Frenicle en 1657

Lord William Brounckner : 1620–1684

Leonard Euler : 1707–1783
Livre d'algèbre en 1770, + fractions continues

Joseph–Louis Lagrange : 1736–1813

1773 : Lagrange et Lessing



Figures 1 and 2. Title pages of two publications from 1773. The first (far left) contains Lagrange's proof of the solvability of Pell's equation, already written and submitted in 1768. The second contains Lessing's discovery of the cattle problem of Archimedes.

La solution triviale $(x, y) = (1, 0)$

Soit d un entier non nul. On s'intéresse à l'équation $x^2 - dy^2 = \pm 1$ en entiers x et y positifs.

Il y a toujours la solution *triviale* $x = 1$, $y = 0$. On cherche s'il y a des solutions non triviales.

Si $d \leq -2$ il n'y en a pas.

Si $d = -1$ il n'y a que $x = 0$, $y = 1$.

On suppose maintenant d positif.

Solutions non triviales

Si d est le carré d'un entier e il n'y a pas de solution non triviale :

$$x^2 - dy^2 = (x - ey)(x + ey) = \pm 1 \Longrightarrow x = 1,\ y = 0.$$

On suppose maintenant que d est positif et n'est pas un carré.

Deux solutions en fournissent une troisième

Partant de deux solutions (x_1, y_1) et (x_2, y_2) en entiers rationnels, on définit (x_3, y_3) par

$$(x_1 + y_1\sqrt{d})(x_2 + y_2\sqrt{d}) = x_3 + y_3\sqrt{d}.$$

Alors on a aussi

$$(x_1 - y_1\sqrt{d})(x_2 - y_2\sqrt{d}) = x_3 - y_3\sqrt{d}.$$

Le produit des membres de gauche

$$(x_1 + y_1\sqrt{d})(x_2 + y_2\sqrt{d})(x_1 - y_1\sqrt{d})(x_2 - y_2\sqrt{d})$$

est ± 1, donc

$$(x_3 + y_3\sqrt{d})(x_3 - y_3\sqrt{d}) = x_3^2 - dy_3^2 = \pm 1,$$

ce qui montre que (x_3, y_3) est aussi une solution.

Un groupe multiplicatif

De la même manière, partant d'une solution (x, y), si on définit (x', y') par

$$(x + y\sqrt{d})^{-1} = x' + y'\sqrt{d},$$

alors

$$(x - y\sqrt{d})^{-1} = x' - y'\sqrt{d},$$

d'où on déduit que (x', y') est de nouveau une solution.

Cela signifie que l'ensemble des solutions en entiers rationnels (positifs ou négatifs) est naturellement muni d'une structure de *groupe multiplicatif*. L'élément neutre est la solution triviale.

Une infinité de solution

S'il y a une solution non triviale (x_1, y_1) en entiers positifs, il y en a une infinité, obtenues en écrivant

$$(x_1 + y_1\sqrt{d})^n = x_n + y_n\sqrt{d}$$

pour $n = 1, 2, \ldots$.
On ordonne les solutions selon $x + y\sqrt{d}$ (il revient au même de prendre l'ordre donné par x, ou celui donné par y). Il existe donc une solution > 1 minimale, on l'appelle la solution fondamentale de l'équation.

Un groupe multiplicatif de rang 1

Si on veut toutes les solutions $(x, y) \in \mathbf{Z} \times \mathbf{Z}$, on fait varier n dans $\mathbf{Z}$ et on considère aussi $(x_1 - y_1\sqrt{d})^n$.

Donc le groupe multiplicatif de toutes les solutions dans $\mathbf{Z} \times \mathbf{Z}$ est un groupe abélien de rang ≤ 1.

La solution $(-1, 0)$ est un élément de torsion d'ordre 2.

L'existence d'une solution autre que $(\pm 1, 0)$ revient à dire que le groupe est de rang 1.

Unités d'un corps de nombres quadratique

Le *théorème des unités de Dirichlet* (dans le cas particulier d'un corps réel quadratique) affirme que le groupe des unités de l'anneau $\mathbf{Z}[\sqrt{d}]$ est de rang 1, ce qui signifie qu'il y a toujours une solution non triviale. Il y en a donc une infinité, données par les puissances de la solution fondamentale.
La démonstration classique utilise la géométrie des nombres de Minkowski).
Le groupe des unités d'un corps de nombres quadratique est de rang 1, isomorphe à $\{\pm 1\} \times \mathbf{Z}$: il existe une unité fondamentale $\epsilon > 1$ telle que toute unité soit de la forme $\pm\epsilon^n$ avec $n \in \mathbf{Z}$.

$+1$ ou -1 ?

• Si la solution fondamentale $x_1^2 - dy_1^2 = \pm 1$ donne le signe $+$, alors l'équation $x^2 - dy^2 = -1$ n'a pas de solution.
(L'unité fondamentale de l'anneau $\mathbf{Z}[\sqrt{d}]$ a pour norme $+1$).

• Si la solution fondamentale $x_1^2 - dy_1^2 = \pm 1$ donne le signe $-$, alors la solution fondamentale de l'équation $x^2 - dy^2 = 1$ est (x_2, y_2) avec $x_2 + y_2\sqrt{d} = (x_1 + y_1\sqrt{d})^2$, donc

$$x_2 = x_1^2 + dy_1^2, \qquad y_2 = 2x_1y_1.$$

Les solutions de l'équation $x^2 - dy^2 = 1$ sont les (x_n, y_n) avec n pair, celles de $x^2 - dy^2 = -1$ sont obtenues avec n impair.
(L'unité fondamentale de l'anneau $\mathbf{Z}[\sqrt{d}]$ a pour norme -1).

Algorithme pour trouver la solution fondamentale

Tout le problème est maintenant de trouver la solution fondamentale.
L'idée est la suivante. Si x, y est une solution, alors l'équation $x^2 - dy^2 = \pm 1$ écrite sous la forme

$$\frac{x}{y} - \sqrt{d} = \pm\frac{1}{y(x + y\sqrt{d})}$$

montre que x/y est une très bonne *approximation rationnelle* de $\sqrt{d}$.
Il y a un algorithme pour construire *les meilleures* approximations rationnelles d'un nombre réel : c'est celui des *fractions continues*.

L'algorithme des fractions continues

Soit $x \in \mathbf{R}$.

- On effectue la division euclidienne de x par 1 :

$$x = [x] + \{x\} \quad \text{avec } [x] \in \mathbf{Z} \text{ et } 0 \leq \{x\} < 1.$$

L'algorithme des fractions continues

Soit $x \in \mathbf{R}$.

- On effectue la division euclidienne de x par 1 :

$$x = [x] + \{x\} \quad \text{avec } [x] \in \mathbf{Z} \text{ et } 0 \leq \{x\} < 1.$$

- Si x est un entier, l'algorithme s'arrête. Si x n'est pas un entier, alors $\{x\} \neq 0$ et on pose $x_1 = 1/\{x\}$, de telle sorte que

$$x = [x] + \frac{1}{x_1} \quad \text{avec } [x] \in \mathbf{Z} \text{ et } x_1 > 1.$$

L'algorithme des fractions continues

Soit $x \in \mathbf{R}$.

- On effectue la division euclidienne de x par 1 :

$$x = [x] + \{x\} \quad \text{avec } [x] \in \mathbf{Z} \text{ et } 0 \leq \{x\} < 1.$$

- Si x est un entier, l'algorithme s'arrête. Si x n'est pas un entier, alors $\{x\} \neq 0$ et on pose $x_1 = 1/\{x\}$, de telle sorte que

$$x = [x] + \frac{1}{x_1} \quad \text{avec } [x] \in \mathbf{Z} \text{ et } x_1 > 1.$$

- Si x_1 est un entier, l'algorithme s'arrête. Si x_1 n'est pas un entier, on pose $x_2 = 1/\{x_1\}$:

$$x = [x] + \cfrac{1}{[x_1] + \cfrac{1}{x_2}} \quad \text{avec } x_2 > 1.$$

Développement en fraction continue

On pose $a_0 = [x]$ et $a_i = [x_i]$ pour $i \geq 1$.

- Alors :

$$x = [x] + \cfrac{1}{[x_1] + \cfrac{1}{[x_2] + \cfrac{1}{\ddots}}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

L'algorithme s'arrête après un nombre fini de pas si et seulement si x est rationnel.

Développement en fraction continue

On pose $a_0 = [x]$ et $a_i = [x_i]$ pour $i \geq 1$.

- Alors :

$$x = [x] + \cfrac{1}{[x_1] + \cfrac{1}{[x_2] + \cfrac{1}{\ddots}}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

L'algorithme s'arrête après un nombre fini de pas si et seulement si x est rationnel.

- On utilise la notation

$$x = [a_0,\ a_1,\ a_2,\ a_3 \ldots]$$

Développement en fraction continue

On pose $a_0 = [x]$ et $a_i = [x_i]$ pour $i \geq 1$.

- Alors :

$$x = [x] + \cfrac{1}{[x_1] + \cfrac{1}{[x_2] + \cfrac{1}{\ddots}}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

L'algorithme s'arrête après un nombre fini de pas si et seulement si x est rationnel.

- On utilise la notation

$$x = [a_0,\ a_1,\ a_2,\ a_3 \ldots]$$

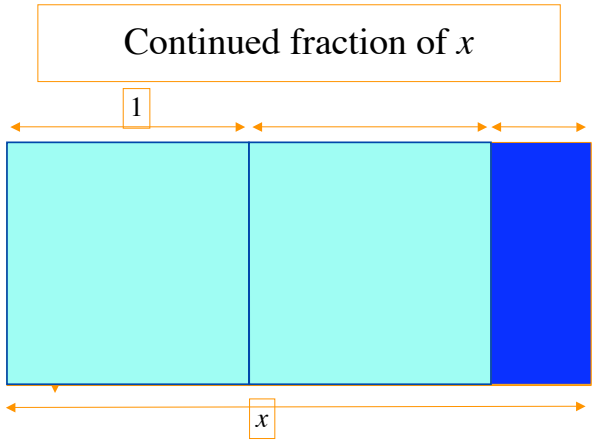
- Remarque : si $a_k \geq 2$, alors
$[a_0,\ a_1,\ a_2,\ a_3, \ldots, a_k] = [a_0,\ a_1,\ a_2,\ a_3, \ldots, a_k - 1, 1]$.

Fraction continue : point de vue géométrique

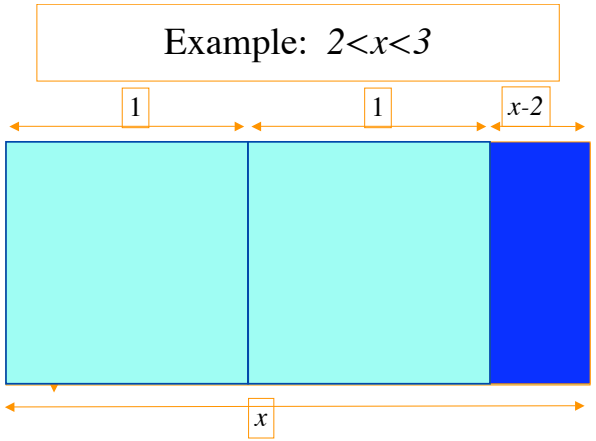
On part d'un rectangle dont les côtés ont pour longueurs 1 and x. La proportion est x.

On le décompose en $[x]$ carrés de côtés 1 et un rectangle pluspetit dont les côtés sont $\{x\} = x - [x]$ et 1.

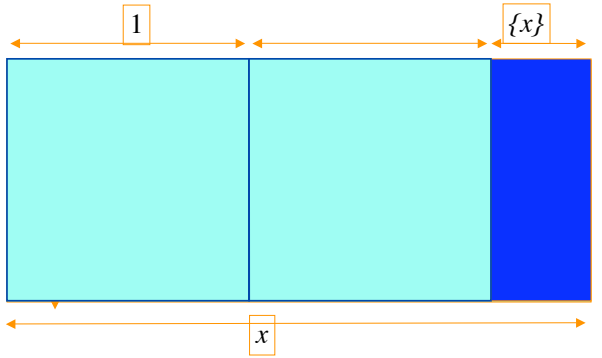
Rectangles ayant pour proportion x



Example : $2 < x < 3$



Nombre de carrés : : $a_0 = [x]$ avec $x = [x] + \{x\}$



Fraction continue : point de vue géométrique

On rappelle que $x_1 = 1/\{x\}$

Les côtés du petit rectangle ont pour proportions x_1.

On répète le processus : on décompose le petit rectangle en $[x_1]$ carrés et un troisième rectangle encore plus petit, donc les côtés ont pour proportion $x_2 = 1/\{x_1\}$.

On obtient ainsi le développement en fraction continue de x.

La suite $a_0, a_1, \ldots$ est donnée par le nombre de carrés à chaque étape.

Exemple : le nombre d'or

Le nombre d'or

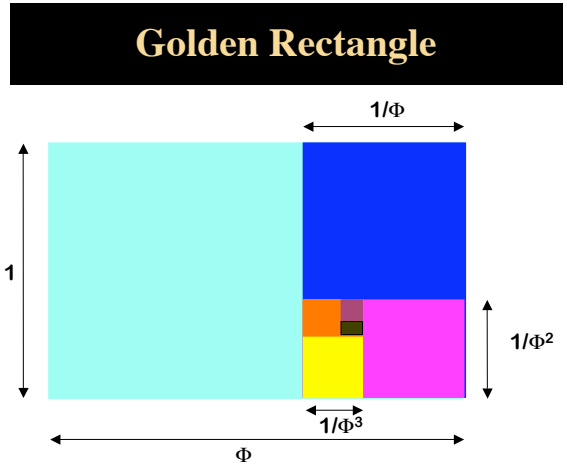
$$\Phi = \frac{1+\sqrt{5}}{2} = 1.6180339887499\ldots$$

vérifie

$$\Phi = 1 + \frac{1}{\Phi}.$$

Donc si on part d'un rectangle dont les longueurs des côtés ont pour proportion le nombre d'or, à chaque étape on obtient un carré et un rectangle plus petit ayant la même proportion.

Le nombre d'or $(1+\sqrt{5})/2 = [1; 1, 1, 1\ldots]$



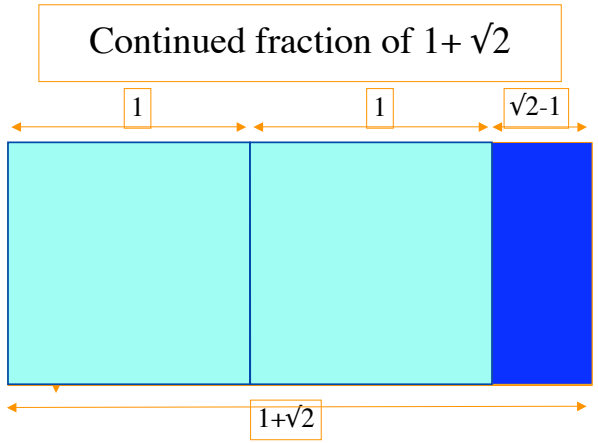
Rectangles ayant pour proportion $1+\sqrt{2}$

$$\sqrt{2} = 1.4142135623731\ldots$$

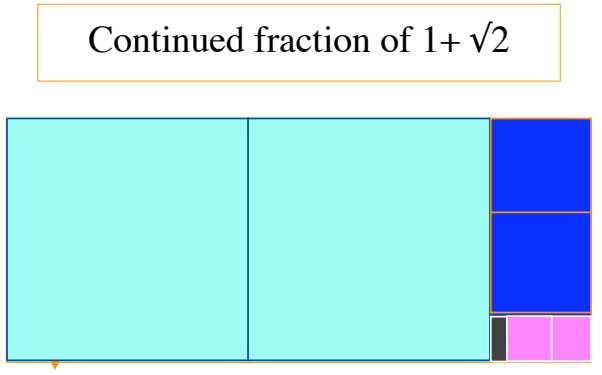
$$1+\sqrt{2} = 2 + \frac{1}{1+\sqrt{2}}$$

Si on part d'un rectangle ayant pour proportion $1+\sqrt{2}$, à chaque étape on trouve deux carrés et un rectangle plus petit dont les côtés sont encore dans la proportion $1+\sqrt{2}$.

Rectangles with proportion $1+\sqrt{2}$



Rectangles ayant pour proportion $1+\sqrt{2}=[2;2,2,2\ldots]$



Démonstrations géométriques d'irrationalité

Quand on part d'un rectangle dont les côtés sont des nombres entiers, à chaque étape les carrés ont des côtés entiers, de plus en plus petits. Donc le processus s'arrête après un nombre fini d'étapes.

De même si on part d'un rectangle ayant des longueurs de côtés en proportion rationnelle, le processus s'arrête après un nombre fini d'étapes. (on se ramène au cas précédent en choisissant bien l'unité de longueur).

Par exemple Φ et $1+\sqrt{2}$ sont des nombres irrationnels, par conséquent $\sqrt{5}$ et $\sqrt{2}$ aussi.

Fractions continues et approximation rationnelle

Pour

$$x=[a_0,\ a_1,\ a_2,\ldots,a_k,\ldots]$$

la suite de nombres rationnels

$$p_k/q_k=[a_0,\ a_1,\ a_2,\ldots,a_k] \qquad (k=1,2,\ldots)$$

donne des approximations du nombre x dont on montre que ce sont *les meilleures* en termes de la qualité de l'approximation comparée à la *taille du dénominateur*.

Fraction continue de la racine d'un entier d

Recette : si d est un entier positif qui n'est pas un carré, la fraction continue de $\sqrt{d}$ est périodique.

Si k est la plus petite période, cette fraction continue s'écrit

$$\sqrt{d} = [a_0\,;\overline{a_1, a_2, \ldots, a_k}],$$

avec $a_k = 2a_0$ et $a_0 = [\sqrt{d}]$.

De plus $(a_1, a_2, \ldots, a_{k-1})$ est un palindrome :

$$a_j = a_{k-j} \quad \text{pour} \quad 1 \leq j < k-1.$$

Le nombre rationnel dont le développement en fraction continue est $[a_0; a_1, \ldots, a_{k-1}]$ est une bonne approximation de $\sqrt{d}$.

Parité de la longueur du palindrome

Si k est pair la solution fondamentale de l'équation $x^2 - dy^2 = 1$ est donnée par la fraction

$$[a_0; a_1, a_2, \ldots, a_{k-1}] = \frac{x_1}{y_1}.$$

Dans ce cas l'équation $x^2 - dy^2 = -1$ n'a pas de solution.

Parité de la longueur du palindrome

Si k est impair la solution fondamentale (x_1, y_1) de l'équation $x^2 - dy^2 = -1$ est donnée par la fraction

$$[a_0; a_1, a_2, \ldots, a_{k-1}] = \frac{x_1}{y_1}$$

et la solution fondamentale (x_2, y_2) de l'équation $x^2 - dy^2 = 1$ par la fraction

$$[a_0; a_1, a_2, \ldots, a_{k-1}, a_k, a_1, a_2, \ldots, a_{k-1}] = \frac{x_2}{y_2}.$$

Remarque. *Que k soit pair ou impair, on obtient aussi la suite $(x_n, y_n)_{n\geq 1}$ de toutes les solutions en répétant $n-1$ fois $a_1, a_2, \ldots, a_k$ suivi de $a_1, a_2, \ldots, a_{k-1}$.*

L'équation de Pell la plus simple $x^2 - 2y^2 = \pm 1$

Euclide, Éléments, II § 10, 300 av. J.C. :

$$17^2 - 2 \cdot 12^2 = 289 - 2 \cdot 144 = 1.$$

$$99^2 - 2 \cdot 70^2 = 9\,801 - 2 \cdot 4900 = 1.$$

$$577^2 - 2 \cdot 408^2 = 332\,929 - 2 \cdot 166\,464 = 1.$$

Triangles Pythagoriciens

Quels sont les triangles rectangles de côtés entiers dont les côtés de l'angle droit sont des entiers consécutifs ?

$$x^2 + y^2 = z^2, \qquad y = x + 1.$$

$$2x^2 + 2x + 1 = z^2$$

$$(2x+1)^2 - 2z^2 = -1$$

$$X^2 - 2Y^2 = -1$$

$1^2 - 2 \cdot 1^2 = -1$
$7^2 - 2 \cdot 5^2 = -1$
$41^2 - 2 \cdot 29^2 = 1681 - 2 \cdot 841 = -1.$

$x^2 - 2y^2 = \pm 1$

$$\sqrt{2} = 1,414213562373095048801688724 2 \ \ldots$$

vérifie

$$\sqrt{2} = 1 + \frac{1}{\sqrt{2}+1}.$$

Donc le développement en fraction continue est périodique de longueur 1 :

$$\sqrt{2} = [1,\ 2,\ 2,\ 2,\ 2,\ 2,\ \ldots] = [1;\ \overline{2}],$$

La solution fondamentale de l'équation $x^2 - 2y^2 = -1$ est $x_1 = 1$, $y_1 = 1$

$$1^2 - 2 \cdot 1^2 = -1,$$

le développement en fraction continue de x_1/y_1 est $[1]$.
L'unité fondamentale de l'anneau $\mathbf{Z}[\sqrt{2}]$ est $1 + \sqrt{2}$, de norme -1.

L'équation de Pell $x^2 - 2y^2 = 1$

La solution fondamentale de l'équation :

$$x^2 - 2y^2 = 1$$

est $x = 3$, $y = 2$, donnée par

$$[1;2] = 1 + \frac{1}{2} = \frac{3}{2}.$$

Le nombre $3 + 2\sqrt{2} = (1+\sqrt{2})^2$ est une unité de norme 1 dans $\mathbf{Z}(\sqrt{2})$.

$x^2 - 3y^2 = 1$

Le développement en fraction continue du nombre

$$\sqrt{3} = 1,732050807568877293527446341 5 \ldots$$

est

$$\sqrt{3} = [1,\ 1,\ 2,\ 1,\ 2,\ 1,\ 2,\ 1,\ 2,\ 1,\ 2,\ 1,\ \ldots] = [1;\ \overline{1,\ 2}],$$

car

$$\sqrt{3} + 1 = 2 + \frac{1}{1 + \frac{1}{\sqrt{3}+1}}.$$

La solution fondamentale de $x^2 - 3y^2 = 1$ est $x = 2$, $y = 1$, correspondant à

$$[1;1] = 1 + \frac{1}{1} = \frac{2}{1}.$$

$x^2 - 3y^2 = 1$

Le nombre $2 + \sqrt{3}$ est une unité de norme 1 dans l'anneau $\mathbf{Z}(\sqrt{3})$:

$$(2 + \sqrt{3})(2 - \sqrt{3}) = 4 - 3 = 1.$$

Il n'y a pas d'unité de norme -1 dans $\mathbf{Z}(\sqrt{3})$.
La période de la fraction continue

$$\sqrt{3} = [1;\ \overline{1,\ 2}]$$

est $[1,\ 2]$ et sa longueur est 2 (donc paire).

Petites valeurs de d

$x^2 - 2y^2 = \pm 1$, $\sqrt{2} = [1; \overline{2}]$, $k = 1$, $(x_1, y_1) = (1, 1)$,
$$1^2 - 2 \cdot 1^2 = -1.$$
$x^2 - 3y^2 = \pm 1$, $\sqrt{3} = [1; \overline{1, 2}]$, $k = 2$, $(x_1, y_1) = (2, 1)$,
$$2^2 - 3 \cdot 1^2 = 1.$$
$x^2 - 5y^2 = \pm 1$, $\sqrt{5} = [2; \overline{4}]$, $k = 1$, $(x_1, y_1) = (2, 1)$,
$$2^2 - 5 \cdot 1^2 = -1.$$
$x^2 - 6y^2 = \pm 1$, $\sqrt{6} = [2; \overline{2, 4}]$, $k = 2$, $(x_1, y_1) = (5, 4)$,
$$5^2 - 6 \cdot 2^2 = 1.$$
$x^2 - 7y^2 = \pm 1$, $\sqrt{7} = [2; \overline{1, 1, 1, 4}]$, $k = 4$, $(x_1, y_1) = (8, 3)$,
$$8^2 - 7 \cdot 3^2 = 1.$$
$x^2 - 8y^2 = \pm 1$, $\sqrt{8} = [2; \overline{1, 4}]$, $k = 2$, $(x_1, y_1) = (3, 1)$,
$$3^2 - 8 \cdot 1^2 = 1.$$

Problème de Brahmagupta (628)

Le développement en fractions continues de $\sqrt{92}$ est

$$\sqrt{92} = [9; \overline{1,\ 1,\ 2,\ 4,\ 2,\ 1,\ 1,\ 18}]$$

La solution fondamentale de l'équation $x^2 - 92y^2 = 1$ est donnée par

$$[9;\ 1,\ 1,\ 2,\ 4,\ 2,\ 1,\ 1] = \frac{1151}{120}.$$

En effet, $1151^2 - 92 \cdot 120^2 = 1\,324\,801 - 1\,324\,800 = 1.$

Équation de Narayana $x^2 - 103y^2 = 1$

$$\sqrt{103} = [10; \overline{6,\ 1,\ 2,\ 1,\ 1,\ 9,\ 1,\ 1,\ 2,\ 1,\ 6,\ 20}]$$

$$[10; 6,\ 1,\ 2,\ 1,\ 1,\ 9,\ 1,\ 1,\ 2,\ 1,\ 6] = \frac{227\,528}{22\,419}$$

Solution fondamentale : $x = 227\,528$, $y = 22\,419$.

$$227\,528^2 - 103 \cdot 22\,419^2 = 51\,768\,990\,784 - 51\,768\,990\,783 = 1.$$

Équation de Bhaskhara II $x^2 - 61y^2 = \pm 1$

$$\sqrt{61} = [7; \overline{1,\ 4,\ 3,\ 1,\ 2,\ 2,\ 1,\ 3,\ 4,\ 1,\ 14}]$$

$$[7; 1, 4, 3, 1, 2, 2, 1, 3, 4, 1] = \frac{29\ 718}{3\ 805}$$

$29\ 718^2 = 883\ 159\ 524, \qquad 61 \cdot 3805^2 = 883\ 159\ 525$
est la solution fondamentale de $x^2 - 61y^2 = -1$.

La solution fondamentale de $x^2 - 61y^2 = 1$ est

$$[7; 1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14, 1, 4, 3, 1, 2, 2, 1, 3, 4, 1] = \frac{1\,766\,319\,049}{226\,153\,980}$$

Correspondance de Fermat avec Brounckner

"*pour ne vous donner pas trop de peine*" (Fermat)

$$X^2 - DY^2 = 1, \text{ avec } D = 61 \text{ et } D = 109.$$

Solutions respectives :

$$(1\,766\,319\,049\ ,\ 226\,153\,980)$$
$$(158\,070\,671\,986\,249,\ 15\,140\,424\,455\,100)$$

$$158\,070\,671\,986\,249\ +\ 15\,140\,424\,455\,100\sqrt{109} = \left(\frac{261 + 25\sqrt{109}}{2}\right)^6.$$

Autour de 2008

Pour $d = 2007$ la plus petite solution est

$$224^2 - 2007 \cdot 5^2 = 1$$

.
Pour $d = 2005$, 2006, 2008 et 2009 les solutions sont gigantesques.

Après, pour 2010, cela redevient raisonnable :

$$269^2 - 2010 \cdot 6^2 = 1$$

.

wims : serveur interactif

reference : `http ://wims.unice.fr/wims/`

Le calcul de la fraction continue est assuré par PARI version 2.2.1.

Equation de Pell pour $x^2 - 2008y^2 = \pm 1$

Développement en fraction continue de *n* = 3832352837/85523139 :

3832352837/85523139 = 44 + 1/1+ 1/4+ 1/3+ 1/1+ 1/1+ 1/6+ 1/1+ 1/9+ 1/11+ 1/9+ 1/1+ 1/6+ 1/1+ 1/1+ 1/3+ 1/5

$$x = 3\,832\,352\,837, \qquad y = 85\,523\,139.$$

$$3\,832\,352\,837^2 - 2008 \cdot 85\,523\,139^2 = 1.$$

Equation de Pell $x^2 - 2009y^2 = \pm 1$

Accueil WIMS Références Aide A propos Aides WIMS

Contfrac

Cette page calcule le développement d'un nombre réel *n* en fraction continue .

Vous pouvez entrer ce nombre *n* par une expression. Exemples d'expressions: élémentaires ou plus approfondis .

Nombre à développer : *n* = sqrt(2009)

Nombre de termes du développement : 100

Signes du développement : +1, +1, +1, +1, ...

Accueil WIMS Aide A propos

Auteur de la page: XIAO Gang

Version 1.01, © 1998-1999 (GNU GPL)

Equation de Pell $x^2 - 2009y^2 = \pm 1$

Accueil WIMS Références Aide A propos Aides WIMS

Contfrac

Développement en fraction continue de *n* = sqrt(2009) :

44.82186966202994080541752372235269285164294092834713219870490838667727930737813252002548011574908974219568282
= 44 + 1/1+ 1/4+ 1/1+ 1/1+ 1/1+ 1/1+ 1/2+ 1/3+ 1/1+ 1/1+ 1/17+ 1/2+ 1/1+ 1/2+ 1/1+ 1/10+ 1/2+ 1/10+ 1/1+ 1/2+ 1/1+ 1/2+
1/17+ 1/1+ 1/1+ 1/3+ 1/2+ 1/1+ 1/1+ 1/1+ 1/1+ 1/4+ 1/1+ 1/88+ 1/1+ 1/4+ 1/1+ 1/1+ 1/1+ 1/1+ 1/2+ 1/3+ 1/1+ 1/1+ 1/17+ 1/2+
1/1+ 1/2+ 1/1+ 1/10+ 1/2+ 1/10+ 1/1+ 1/2+ 1/1+ 1/2+ 1/17+ 1/1+ 1/1+ 1/3+ 1/2+ 1/1+ 1/1+ 1/1+ 1/1+ 1/4+ 1/1+ 1/88+ 1/1+
1/4+ 1/1+ 1/1+ 1/1+ 1/1+ 1/2+ 1/3+ 1/1+ 1/1+ 1/17+ 1/2+ 1/1+ 1/2+ 1/1+ 1/10+ 1/2+ 1/10+ 1/1+ 1/2+ 1/1+ 1/2+ 1/17+ 1/1+
1/1+ 1/3+ 1/2+ 1/1+ 1/1+ 1/1+ 1/1+ . . .

Avec javascript, placer la souris sur un dénominateur fera afficher le convergent du terme correspondant (précision limitée) :

Solution fondamentale de l'équation $x^2 - 2009y^2 = \pm 1$

$$x = 141\,012\,534\,067\,201, \qquad y = 3\,146\,065\,416\,960$$

$$141\,012\,534\,067\,201 - 2009 \cdot 3\,146\,065\,416\,960 = 1$$

Retour sur le problème d'Archimède

$$x^2 - 410\,286\,423\,278\,424 y^2 = 1$$

Calcul de la fraction continue de $\sqrt{410\,286\,423\,278\,424}$.

En 1867, C.F. Meyer a effectué les 240 premiers pas de l'algorithme mais a abandonné.

La *longueur de la période* a été calculée depuis : elle est de $203\,254$.

Solution par Amthor – Lenstra

$d = (2 \cdot 4657)^2 \cdot d' \qquad d' = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 29 \cdot 353.$

Longueur de la période pour $\sqrt{d'}$: 92.

Unité fondamentale : $u = x' + y'\sqrt{d'}$

$$u = \big(300\,426\,607\,914\,281\,713\,365 \cdot \sqrt{609} + 84\,129\,507\,677\,858\,393\,258\sqrt{7766}\big)^2$$

Solution fondamentale de l'équation d'Archimède :

$$x_1 + y_1\sqrt{d} = u^{2329}.$$

$p = 4657$, $(p+1)/2 = 2329 = 17 \cdot 137$.

Longueur de la période et régulateur

Estimation de la longueur L_d de la période en fonction de d :

$$\frac{\log 2}{2} L_d \leq R_d \leq \frac{\log(4d)}{2} L_d, \qquad R_d = \log(x_1 + y_1\sqrt{d})$$

avec

$$\log(2\sqrt{d}) < R_d < \sqrt{d}\big(\log(4d) + 2\big).$$

Toute méthode de solution de l'équation de Pell–Fermat qui nécessite de donner les chiffres de la solution fondamentale a une complexité exponentielle.

R_d est le régulateur du noyau de la norme

$$(\mathbf{Z}[\sqrt{d}])^\times \to \mathbf{Z}^\times = \{\pm 1\}$$

Variétés Riemanniennes de courbure négative

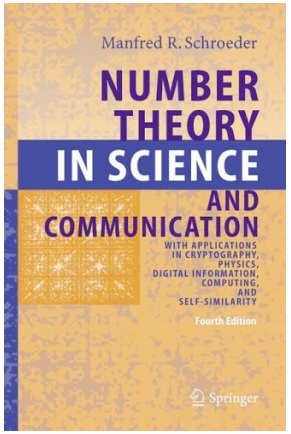
Variétés arithmétiques
Nicolas Bergeron (Paris VI) : "Sur la topologie de certains espaces provenant de constructions arithmétiques"

Substitutions de mots de Christoffel

J. Riss, 1974
J-P. Borel et F. Laubie, Quelques mots sur la droite projective réelle ; Journal de Théorie des Nombres de Bordeaux, **5** 1 (1993), 23–51

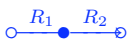
Number Theory in Science and communication

M.R. Schroeder.
Number theory in science and communication :
with applications in cryptography, physics, digital information, computing and self similarity
Springer series in information sciences **7** 1986.
4th ed. (2006) 367 p.



Réseaux électriques

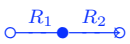
- La résistance d'un réseau en série



est la somme $R_1 + R_2$.

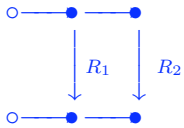
Réseaux électriques

- La résistance d'un réseau en série



est la somme $R_1 + R_2$.

- La résistance d'un réseau en parallèle R

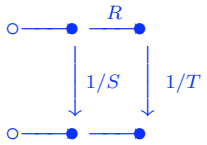


satisfait

$$\frac{1}{R} = \frac{1}{R_1} + \frac{1}{R_2}.$$

Réseaux et fractions continues

La résistance U du circuit



est donnée par

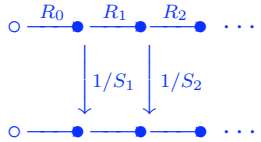
$$U = \cfrac{1}{S + \cfrac{1}{R + \cfrac{1}{T}}}$$

Réseaux électriques, fractions continues et décomposition d'un carré en carrés

- La résistance du réseau suivant est donnée par une fraction continue

$$[R_0; S_1, R_1, S_2, R_2 \dots]$$

pour le circuit



R_i : résistances en séries

$1/S_j$: résistances en parallèle

- Par exemple, pour $R_i = S_j = 1$, on obtient les quotients de nombres de Fibonacci consécutifs.

Réseaux électriques, fractions continues et décomposition d'un carré en carrés

- La résistance du réseau suivant est donnée par une fraction continue

$$[R_0; S_1, R_1, S_2, R_2 \dots]$$

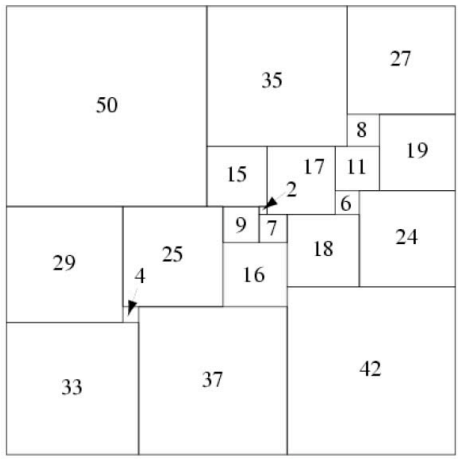
pour le circuit

R_i : résistances en séries

$1/S_j$: résistances en parallèle

- Par exemple, pour $R_i = S_j = 1$, on obtient les quotients de nombres de Fibonacci consécutifs.
- Les réseaux électriques et les fractions continues ont été utilisés pour trouver la première solution du problème de décomposition d'un carré entier en réunion disjointe de carrés entiers tous distincts.

Quadrature du carré



21-*square perfect square*

There is a unique simple perfect square of order 21 (the lowest possible order), discovered in 1978 by A. J. W. Duijvestijn (Bouwkamp and Duijvestijn 1992). It is composed of 21 squares with total side length 112, and is illustrated above.

15 janvier 2009

Cours de Théorie des Nombres MM020

L'équation dite de Pell–Fermat

$x^2 - dy^2 = \pm 1$

Michel Waldschmidt

Institut de Mathématiques de Jussieu & CIMPA

http ://www.math.jussieu.fr/∼miw/