24/12/2017

L'équation de Brahmagupta – Fermat – Pell

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

par

Michel Waldschmidt

Université Pierre et Marie Curie (Paris 6) France

http://www.imj-prg.fr/~michel.waldschmidt/

L'équation de Brahmagupta – Fermat – Pell

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

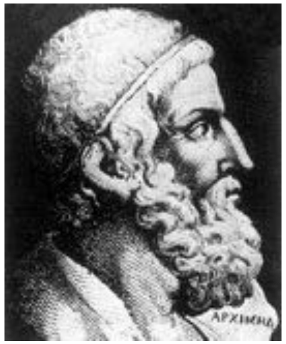
$$1\,151^2 - 92 \cdot 120^2 = 1, \qquad 29\,718^2 - 61 \cdot 3\,805^2 = -1$$

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

$$8(T+X)+1 \quad \text{est un carré} \quad (2m+1)^2=V^2.$$

Équation de Pell associée au problème d'Archimède

En écrivant $T+X=Wk$ avec $W=7\cdot 353\cdot 4657$, on obtient

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

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

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

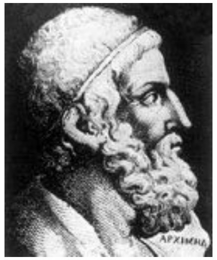
$$D=(2\cdot 4657)^2\cdot 4\,729\,494=410\,286\,423\,278\,424.$$

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: lettre d'Archimèdes à Eratosthènes

Archimèdes
(287 BC –212 BC)



Eratosthènes de Cyrène
(276 BC - 194 BC)

Histoire

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 Archimedes 251 BC, Amer. Math. Monthly **2** (1895), 140–141.
Calcul des 30 premiers et 12 derniers chiffres décimaux. The Hillsboro, Illinois, Mathematical Club, A.H. Bell, E. Fish, G.H. Richard – 4 années de calcul.

"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).

$$77602714 \star\star\star\star\star\star 37983357 \star\star\star\star\star\star 55081800$$

où chacun des douze symboles $\star$ représente $17\,210$ 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*

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

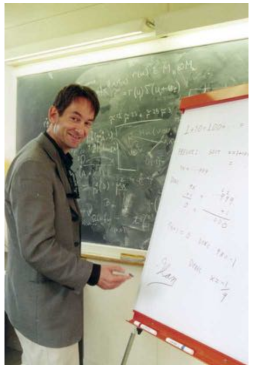
$10^{10^{10}}$ a $1 + 10^{10}$ chiffres décimaux (10 milliards).

Ilan Vardi

http://www.math.nyu.edu/ crorres/Archimedes/Cattle/Solution1.html

$$\left\lfloor \tfrac{25194541}{184119152} (109931986732829734979866232821433543901088049 + 50549485234315033074477819735540408986340\sqrt{4729494})^{4658} \right\rfloor$$

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



Solution du problème d'Archimède

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 (598 – 670)

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* – identité de Brahmagupta

$$(a^2 - db^2)(x^2 - dy^2) = (ax + dby)^2 - d(ay + bx)^2.$$

http://mathworld.wolfram.com/BrahmaguptasProblem.html
http://www-history.mcs.st-andrews.ac.uk/HistTopics/Pell.html

Bhaskara II = Bhaskaracharya (1114 - 1185)

Lilavati Ujjain (Inde)

(*Bijaganita*, 1150)

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

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

Méthode cyclique (*Chakravala*): fournit une solution à l'équation de Pell $x^2 - dy^2 = 1$ à partir d'une solution de $a^2 - db^2 = k$ quand k est *petit*.
http://www-history.mcs.st-andrews.ac.uk/HistTopics/Pell.html

Narayana (14-ième siècle)

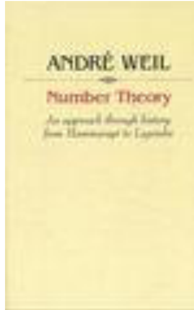
Narayana cows (*Tom Johnson*)

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

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

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:

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

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

Écrivons

$$x^2 - dy^2 = (x + y\sqrt{d})(x - y\sqrt{d}).$$

Deux solutions en produisent une troisième

La relation

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

s'écrit

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

Théorème.

Étant données deux solutions (x_1, y_1) et (x_2, y_2) en entiers rationnels,

$$x_1^2 - dy_1^2 = \pm 1, \quad x_2^2 - dy_2^2 = \pm 1,$$

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 (x_3, y_3) est encore une solution.

Deux solutions en fournissent une troisième

Démonstration.

De

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

on déduit

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

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 $(x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = \pm 1$, 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 encore une solution. $\square$

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

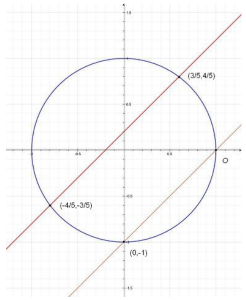
$$(x - y\sqrt{d})^{-1} = x' - y'\sqrt{d},$$

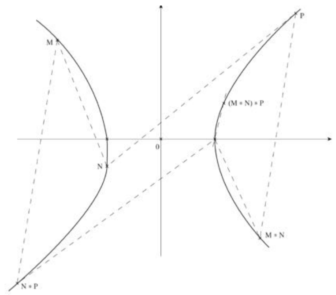
d'où on déduit que (x', y') est de nouveau une solution.

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.

Loi de groupe sur une conique

La courbe d'équation $x^2 - Dy^2 = 1$ est une conique (hyperbole), et sur toute conique il y a une loi de groupe qui peut être décrite géométriquement. L'associativité se démontre en utilisant le théorème de Pascal.





Le groupe des solutions $(x, y) \in \mathbf{Z} \times \mathbf{Z}$

Soit G l'ensemble des $(x, y) \in \mathbf{Z}^2$ vérifiant $x^2 - dy^2 = \pm 1$. Muni de la loi donnée par la bijection

$$(x, y) \in G \longmapsto x + y\sqrt{d} \in \mathbf{Z}[\sqrt{d}]^\times$$

G devient un groupe multiplicatif (*transport de structure*).

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

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).

Donc, s'il existe une solution > 1, alors il en existe une minimale, on l'appelle *la solution fondamentale* de l'équation.

Deux théorèmes

Soit d un entier positif qui n'est pas un carré.

Théorème.
Il existe une solution non triviale (x, y) *en entiers positifs à l'équation* $x^2 - dy^2 = \pm 1$.

Par conséquent il y a une infinité de solutions en entiers rationnels positifs. Il en existe une minimale, la solution fodamentale (x_1, y_1). Pour tout n in $\mathbf{Z}$ et tout choix du signe $\pm$, on obtient une solution (x, y) en entiers rationnels en écrivant $(x_1 + y_1\sqrt{d})^n = x + \sqrt{d}y$.

Théorème.
Pour toute solution en entiers rationnels de l'équation $x^2 - dy^2 = \pm 1$, *il existe un entier rationnel* n *dans* $\mathbf{Z}$ *et un signe* $\pm$, *tel que* $x + \sqrt{d}y = \pm(x_1 + y_1\sqrt{d})^n$.

Le groupe G a un rang ≤ 1

Soit φ l'homomorphisme

$$(x, y) \in G \longmapsto \left(\log|x + y\sqrt{d}|\ ,\ \log|x - y\sqrt{d}|\right) \in \mathbf{R}^2.$$

Le noyau de φ est le sous-groupe de torsion $\{(\pm 1, 0)\}$ de G. L'image $\mathcal{G}$ de G sous φ est un sous-groupe discret de la droite $\{(t_1, t_2) \in \mathbf{R}^2\ ;\ t_1 + t_2 = 0\}$. Donc il existe $u \in \mathcal{G}$ tel que $\mathcal{G} = \mathbf{Z}u$.

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

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

$+1$ 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.

- 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.

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:

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

• 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

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

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

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

Développement en fraction continue

On pose $a_0 = \lfloor x \rfloor$ et $a_i = \lfloor x_i \rfloor$ pour $i \geq 1$.
• Alors:

$$x = \lfloor x \rfloor + \cfrac{1}{\lfloor x_1 \rfloor + \cfrac{1}{\lfloor x_2 \rfloor + \cfrac{1}{\ddots}}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

L'algorithme s'arrête après un nombre fini de pas si et seulement si x est rationnel.
• On utilise la notation

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

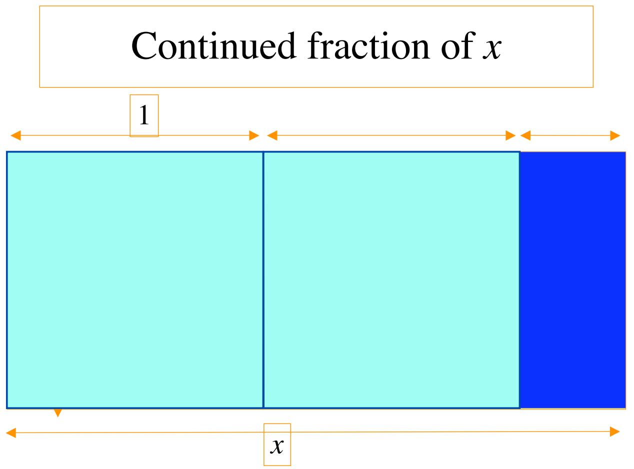
• Remarque: si $a_k \geq 2$, alors
$[a_0,\ a_1,\ a_2,\ a_3, \ldots, a_k] = [a_0,\ a_1,\ a_2,\ a_3, \ldots, a_k - 1, 1]$.

Fraction continue:
point de vue géométrique

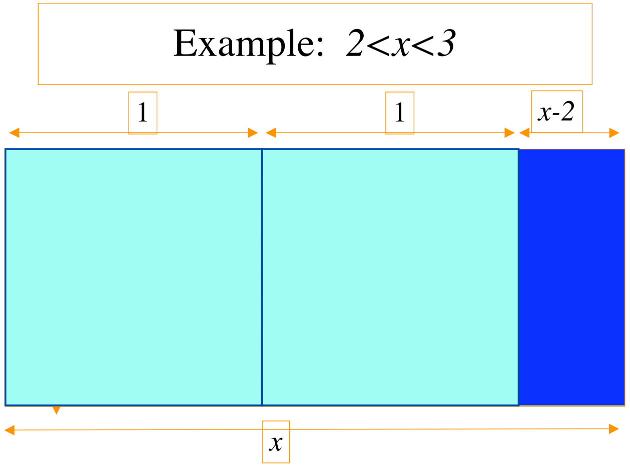
On part d'un rectangle dont les côtés ont pour longueurs 1 and x. La proportion est x.

On le décompose en $\lfloor x \rfloor$ carrés de côtés 1 et un rectangle plus petit dont les côtés sont $\{x\} = x - \lfloor x \rfloor$ et 1.

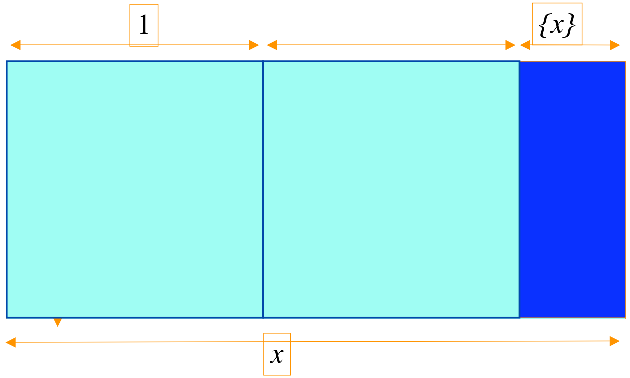
Rectangles ayant pour proportion x



Example: $2 < x < 3$



Nombre de carrés:: $a_0 = \lfloor x \rfloor$ avec $x = \lfloor x \rfloor + \{x\}$



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 $\lfloor x_1 \rfloor$ 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

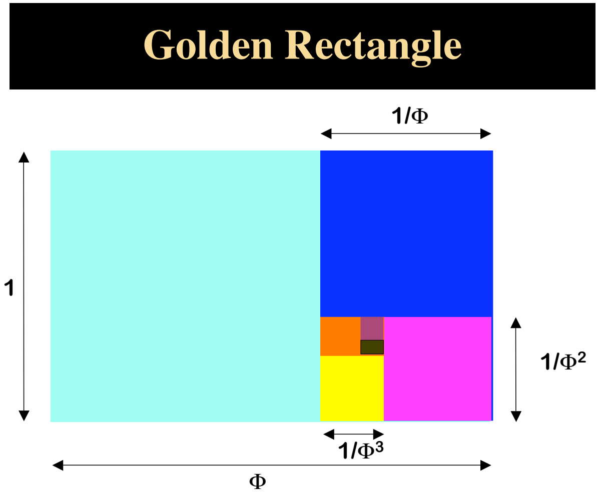
$$\Phi = \frac{1+\sqrt{5}}{2} = 1.6180339887499\ldots$$

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 $(1+\sqrt{5})/2 = [1, 1, 1, 1 \ldots]$



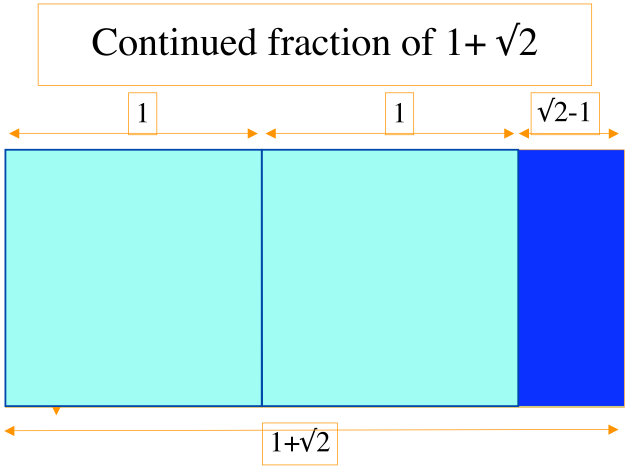
Rectangles ayant pour proportion $1+\sqrt{2}$

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

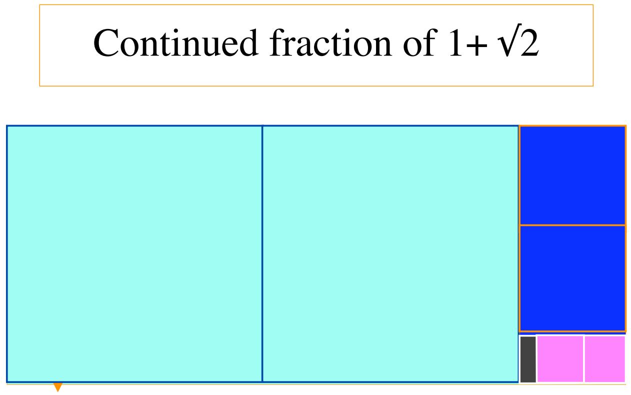
$$1+\sqrt{2} = 2 + \frac{1}{1+\sqrt{2}}$$

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 de 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

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

la suite de nombres rationnels

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

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

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

avec $a_k = 2a_0$ et $a_0 = \lfloor \sqrt{d} \rfloor$.

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

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

Le nombre rationnel dont le développement en fraction continue est $[a_0, a_1, \dots, a_{k-1}]$ 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

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

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

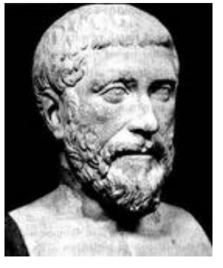
Euclide, Éléments, II § 10, 300 av. J.C.:

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

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

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

Triangles Pythagoriciens



Pythagoras of Samos
about 569 BC - about 475 BC

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

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

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

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

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

$$(X, Y) = \quad (1,1), \quad (7,5), \quad (41,29)\ldots$$

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

$$\sqrt{2} = 1,4142135623730950488016887242\ \ldots$$

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'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

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

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

Le développement en fraction continue du nombre

$$\sqrt{3} = 1,7320508075688772935274463415\ldots$$

est

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

car

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

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

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

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

La solution fondamentale de l'équation $x^2 - 3y^2 = 1$ est $(x, y) = (2, 1)$:

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

Il n'y a pas de solution à l'équation $x^2 - 3y^2 = -1$.
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

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

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 :

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

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

2015, 2016 et 2018

Pour $d = 2015$,

$$\sqrt{2015} = [44,\ \overline{1,\ 7,\ 1,\ 88}], \qquad [44,\ 1,\ 7,\ 1] = \frac{404}{9}$$

la longueur de la période est 4, la solution fondamentale est

$$404^2 - 2015 \cdot 9^2 = 163\,216 - 163\,215 = 1.$$

Pour $d = 2016$,

$$\sqrt{2016} = [44,\ \overline{1,\ 8,\ 1,\ 88}], \qquad [44,\ 1,\ 8,\ 1] = \frac{449}{10},$$

la longueur de la période est 4, la solution fondamentale est

$$449^2 - 2016 \cdot 10^2 = 201\,601 - 201\,600 = 1.$$

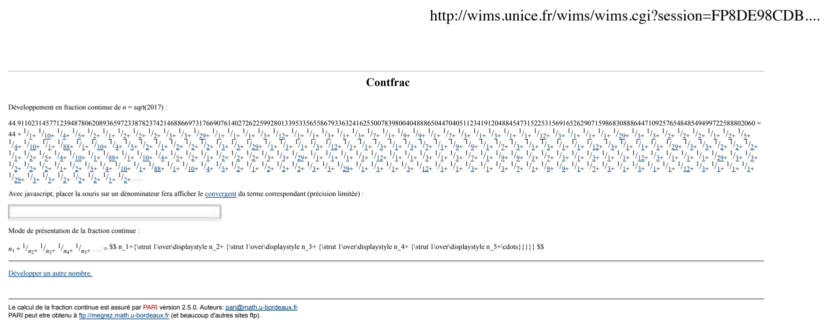
Pour $d = 2018$,

$$\sqrt{2018} = [44,\ \overline{1,\ 11,\ 1,\ 5,\ 2,\ 44,\ 2,\ 5,\ 1,\ 11,\ 1,\ 88}],$$

longueur de la période 12.
Solution fondamentale $x = 56\,280\,003$, $y = 1\,252\,834$.

wims: WWW Interactive Multipurpose Server

Exercice: pour 2017, calculer la longueur de la période et le nombre de chiffres décimaux de la solution fondamentale.
Indication: référence: `http://wims.unice.fr/wims/`
The continued fraction is computed by PARI version 2.2.1.



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:

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

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

Taille de la solution fondamentale

$$2\sqrt{d} < x_1 + y_1\sqrt{d} < (4e^2 d)^{\sqrt{d}}.$$

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

Longueur L_d de la période:

$$\frac{\log 2}{2} L_d \le \log(x_1 + y_1\sqrt{d}) \le \frac{\log(4d)}{2} L_d.$$

Problème 999 de David Masser

Trouver un polynôme quadratique $F(X,Y)$ à coefficients dans $\mathbf{Z}$ de valeurs absolues au plus 999 (i.e. ont au plus trois chiffres) tels que la plus petite solution entière non triviale de l'équation $F(X,Y) = 0$ soit aussi grande que possible.

Daniel M. Kornhauser, *On the smallest solution to the general binary quadratic Diophantine equation.* Acta Arith. **55** (1990), 83-94.

La plus petite solution peut-être aussi grande que $2^{H/5}$, et

$$2^{999/5} = 1.39\ldots 10^{60}.$$

Équation de Pell pour 991:

$$379\,516\,400\,906\,811\,930\,638\,014\,896\,080^2 -$$

$$991 \times 12\,055\,735\,790\,331\,359\,447\,442\,538\,767^2 = 1.$$

Variétés arithmétiques

Soit D un entier non carré. La forme quadratique $x^2 - Dy^2$ est anisotrope sur $\mathbf{Q}$.
Notons $\mathcal{G} = \{(x,y) \in \mathbf{R}^2 \; ; \; x^2 - Dy^2 = 1\}$.

L'application

$$\begin{array}{ccc} \mathcal{G} & \longrightarrow & \mathbf{R}^\times \\ (x,y) & \longmapsto & t = x + y\sqrt{D} \end{array}$$

est bijective: pour écrire la bijection réciproque on pose $u = 1/t$, $2x = t + u$, $2y\sqrt{D} = t - u$, de sorte que $t = x + y\sqrt{D}$ et $u = x - y\sqrt{D}$.

Variétés arithmétiques

Par transport de structure, cela munit

$$\mathcal{G} = \{(x,y) \in \mathbf{R}^2 \; ; \; x^2 - Dy^2 = 1\}$$

d'une structure de groupe multiplicatif, isomorphe à $\mathbf{R}^\times$, pour lequel

$$\begin{array}{ccc} \mathcal{G} & \longrightarrow & \mathrm{GL}_2(\mathbf{R}) \\ (x,y) & \longmapsto & \begin{pmatrix} x & Dy \\ y & x \end{pmatrix}. \end{array}$$

est un homomorphisme injectif de groupes. On note $G(\mathbf{R})$ son image, qui est donc isomorphe à $\mathbf{R}^\times$.

Variétés arithmétiques

Une matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ préserve la forme quadratique $x^2 - Dy^2$ si et seulement si

$$(ax + by)^2 - D(cx + dy)^2 = x^2 - Dy^2,$$

ce qui s'écrit

$$a^2 - Dc^2 = 1, \quad b^2 - Dd^2 = D, \quad ab = cdD.$$

Il en résulte que le groupe des matrices de déterminant 1 à coefficients dans $\mathbf{Z}$ qui préservent la forme quadratique $x^2 - Dy^2$ est le groupe

$$G(\mathbf{Z}) = \left\{ \begin{pmatrix} a & Dc \\ c & a \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Z}) \right\}.$$

Variétés Riemanniennes de courbure négative

D'après les travaux de Siegel, Harish–Chandra, Borel et Godement, le quotient de $G(\mathbf{R})$ par $G(\mathbf{Z})$ est compact. Donc $G(\mathbf{Z})$ est infini (de rang 1 sur $\mathbf{Z}$), ce qui signifie qu'il y a une infinité de solution entières à l'équation $a^2 - Dc^2 = 1$.

Il ne s'agit pas d'une nouvelle démonstration de ce fait, mais plutôt d'une interprétation et d'une généralisation.

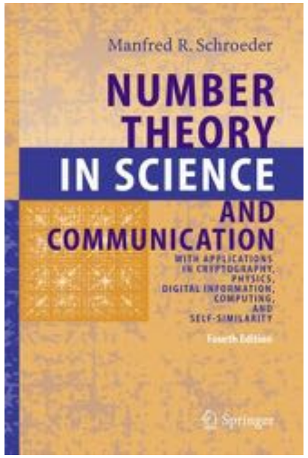
Nicolas Bergeron (Paris VI): "Sur la topologie de certains espaces provenant de constructions arithmétiques"
" *Sur la forme de certains espaces provenant de constructions arithmétiques*, Images des Mathématiques, (2004).
`http://www.math.jussieu.fr/~bergeron/`

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

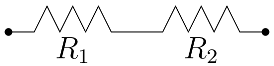
Number Theory in Science and communication

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.

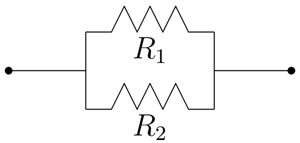


Réseaux électriques

- La résistance d'un réseau en série



est la somme $R_1 + R_2$.
- La resistance R d'un réseau en parallèle

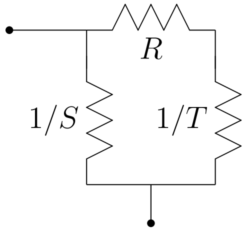


vérifie

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

Réseaux électriques et fractions continues

La resistance U du circuit

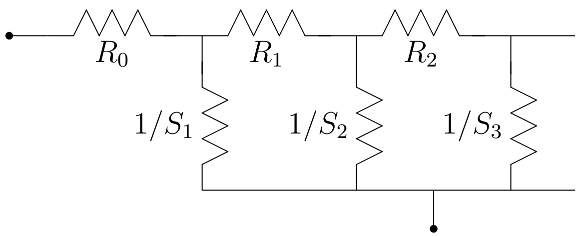


est donnée par

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

Décomposition d'un carré en carré

- Pour le réseau

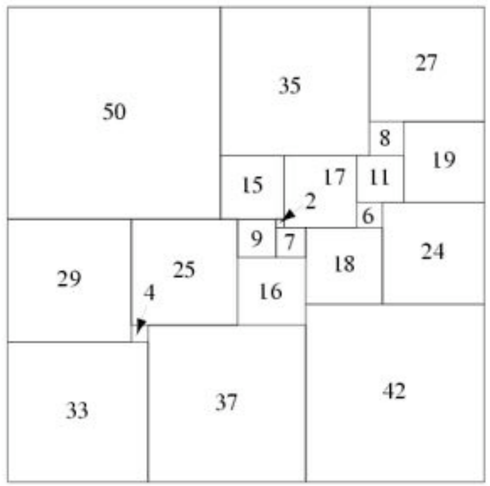


la résistance est donnée par la fraction continue

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

- Les réseaux électriques et les fractions continues ont été utilisés pour trouver la première solution au 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.

L'équation de Brahmagupta – Fermat – Pell

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

par

Michel Waldschmidt

Université Pierre et Marie Curie (Paris 6) France

http://www.imj-prg.fr/~michel.waldschmidt/