On the Archimedes Cattle Problem and the Brahmagupta–Fermat–Pell Equation

Michel Waldschmidt

Professeur Émérite, Sorbonne Université
Institut de Mathématiques de Jussieu Paris Rive Gauche
http://www.imj-prg.fr/~michel.waldschmidt/

On the Brahmagupta–Fermat–Pell equation

The equation $x^2 - dy^2 = \pm 1$, where the unknowns x and y are positive integers while d is a fixed positive integer which is not a square, has been mistakenly called with the name of Pell by Euler. It was investigated by Indian mathematicians since Brahmagupta (628) who solved the case $d = 92$, next by Bhaskara II (1150) for $d = 61$ and Narayana (during the 14-th Century) for $d = 103$. The smallest solution of $x^2 - dy^2 = 1$ for these values of d are respectively

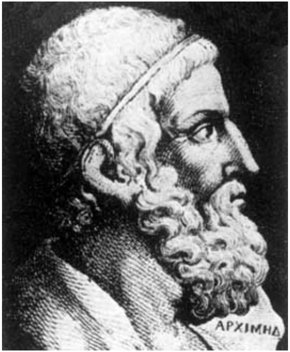
$$1\,151^2 - 92 \cdot 120^2 = 1, \qquad 1\,766\,319\,049^2 - 61 \cdot 226\,153\,980^2 = 1$$

and

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

hence they have not been found by a brute force search !
After a short introduction to this long story, we explain the connection with Diophantine approximation and continued fractions, next we say a few words on more recent developments of the subject.

Archimedes cattle problem



The sun god had a herd of cattle consisting of bulls and cows, one part of which was white, a second black, a third spotted, and a fourth brown.

The Bovinum Problema

Among the bulls, the number of white ones was one half plus one third the number of the black greater than the brown.

The number of the black, one quarter plus one fifth the number of the spotted greater than the brown.

The number of the spotted, one sixth and one seventh the number of the white greater than the brown.

First system of equations

$B =$ white bulls, $N =$ black bulls,
$T =$ brown bulls , $X =$ spotted bulls

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

Up to a multiplicative factor, the solution is

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

The Bovinum Problema

Among the cows, the number of white ones was one third plus one quarter of the total black cattle.

The number of the black, one quarter plus one fifth the total of the spotted cattle ;

The number of spotted, one fifth plus one sixth the total of the brown cattle ;

The number of the brown, one sixth plus one seventh the total of the white cattle.

What was the composition of the herd ?

Second system of equations

$b =$ white cows, $n =$ black cows,
$t =$ brown cows, $x =$ spotted cows

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

Since the solutions b, n, x, t are requested to be integers, one deduces

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

Archimedes Cattle Problem

If thou canst accurately tell, O stranger, the number of cattle of the Sun, giving separately the number of well-fed bulls and again the number of females according to each colour, thou wouldst not be called unskilled or ignorant of numbers, but not yet shalt thou be numbered among the wise.

The Bovinum Problema

But come, understand also all these conditions regarding the cattle of the Sun.

When the white bulls mingled their number with the black, they stood firm, equal in depth and breadth, and the plains of Thrinacia, stretching far in all ways, were filled with their multitude.

Again, when the yellow and the dappled bulls were gathered into one herd they stood in such a manner that their number, beginning from one, grew slowly greater till it completed a triangular figure, there being no bulls of other colours in their midst nor none of them lacking.

Arithmetic constraints

$$B + N = \text{a square},$$
$$T + X = \text{a triangular number}.$$

As a function of the integer k, we have $B + N = 4Ak$ with $A = 3 \cdot 11 \cdot 29 \cdot 4657$ squarefree. Hence $k = AU^2$ with U an integer. On the other side if $T + X$ is a triangular number $(= m(m+1)/2)$, then

$$8(T + X) + 1 \quad \text{is a square} \quad (2m+1)^2 = V^2.$$

Pell's equation associated with the cattle problem

Writing $T + X = Wk$ with $W = 7 \cdot 353 \cdot 4657$, we get

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

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

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

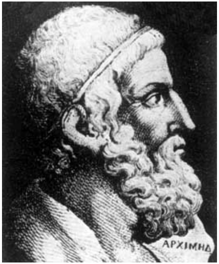
$$D = (2 \cdot 4657)^2 \cdot 4\,729\,494 = 410\,286\,423\,278\,424.$$

Cattle problem

If thou art able, O stranger, to find out all these things and gather them together in your mind, giving all the relations, thou shalt depart crowned with glory and knowing that thou hast been adjudged perfect in this species of wisdom.

History : letter from Archimedes to Eratosthenes

Archimedes
(287 BC –212 BC)



Eratosthenes of Cyrene
(276 BC - 194 BC)

History (continued)

Odyssey of Homer - the Sun God Herd

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

C.F. Meyer, 1867

A. Amthor, 1880 : the smallest solution has $206\,545$ digits, starting with 776.
B. Krumbiegel and A. Amthor, Das Problema Bovinum des Archimedes, Historisch-literarische Abteilung der Zeitschrift für Mathematik und Physik, **25** *(1880), 121–136, 153–171.*

History (continued)

A.H. Bell, The "Cattle Problem" by Archimedes 251 BC, Amer. Math. Monthly **2** (1895), 140–141.
Computation of the first 30 and last 12 decimal digits. The Hillsboro, Illinois, Mathematical Club, A.H. Bell, E. Fish, G.H. Richard – 4 years of computations.

"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

History (continued)

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.

The solution

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

Print out of the smallest solution with $206\,545$ decimal digits : 47 pages (H.G. Nelson, 1980).

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

where each of the twelve symbols $\star$ represents $17\,210$ digits.

Large numbers

A number written with only 3 digits, but having nearly 370 millions decimal digits

The number of decimal digits of 9^{9^9} *is*

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

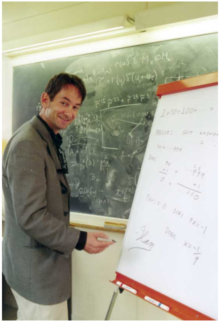
$10^{10^{10}}$ has $1 + 10^{10}$ decimal digits.

Ilan Vardi

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

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

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



A simple solution to Archimedes' cattle problem

Antti Nygrén, "A simple solution to Archimedes' cattle problem", University of Oulu Linnanmaa, Oulu, Finland Acta Universitatis Ouluensis Scientiae Rerum Naturalium, 2001.

50 first digits
$77602714064868182695302328332138866642323224059233$

50 last digits :
$05994630144292500354883118973723406626719455081800$

Solution of Pell's equation

H.W. Lenstra Jr

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

http://www.ams.org/notices/200202/fea-lenstra.pdf

Solution of Archimedes Problem

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.

Brahmagupta (598 – 670)

Brahmasphutasiddhanta : Solve in integers the equation

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

The smallest solution is

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

Composition method : *samasa* – Brahmagupta identity

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

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

Bhaskara II or Bhaskaracharya (1114 - 1185)

Lilavati Ujjain (India)

(*Bijaganita*, 1150)

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

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

Cyclic method (*Chakravala*) : produce a solution to Pell's equation $x^2 - dy^2 = 1$ starting from a solution to $a^2 - db^2 = k$ with a *small* k.

http://www-history.mcs.st-andrews.ac.uk/HistTopics/Pell.html

Narayana Pandit ∼ 1340 – ∼ 1400

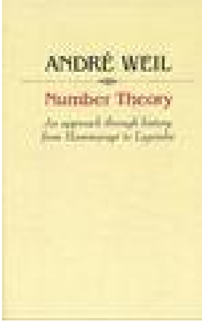
Narayana cows (*Tom Johnson*)

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

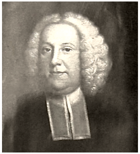
$$x = 227\,528, \qquad y = 22\,419.$$

Reference to Indian mathematics

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



History

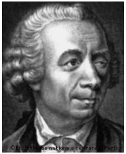


John Pell
1610 – 1685

Pierre de Fermat
1601 – 1665

Lord William Brouncker
1620 – 1684

Joseph–Louis Lagrange
1736 – 1813

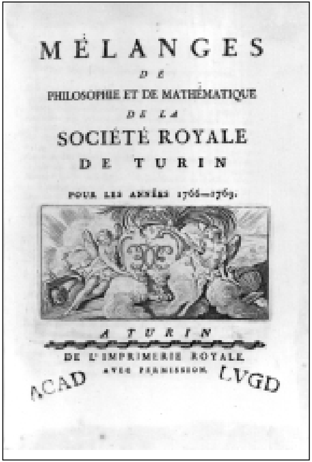


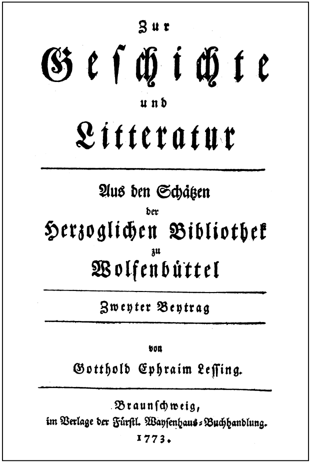
Leonard Euler
1707 – 1783

Letter of Fermat to Frenicle in 1657

Euler : *Book of algebra in 1770 + continued fractions*

1773 : Lagrange and Lessing


MÉLANGES
DE
PHILOSOPHIE ET DE MATHÉMATIQUE
DE LA
SOCIÉTÉ ROYALE
DE TURIN
POUR LES ANNÉES 1766–1769.
A TURIN
DE L'IMPRIMERIE ROYALE
AVEC PERMISSION.
ACAD LVGD


Zur
Geschichte
und
Litteratur
Aus den Schätzen
der
Herzoglichen Bibliothek
zu
Wolfenbüttel
Zweyter Beytrag
von
Gotthold Ephraim Lessing.
Braunschweig,
im Verlage der Fürstl. Waysenhaus-Buchhandlung.
1773.

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.

The trivial solution $(x, y) = (1, 0)$

Let d be a nonzero integer. Consider the equation $x^2 - dy^2 = \pm 1$ in positive integers x and y.

The *trivial* solution is $x = 1$, $y = 0$. We are interested with nontrivial solutions.

In case $d \leq -2$, there is no nontrivial solution to $x^2 + |d|y^2 = \pm 1$.

For $d = -1$ the only non–trivial solution to $x^2 + y^2 = \pm 1$ is $x = 0$, $y = 1$.

Assume now d is positive.

Nontrivial solutions

If $d = e^2$ is the square of an integer e, there is no nontrivial solution :

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

Assume now d is positive and not a square.

Let us write

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

Finding solutions

The relation

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

is equivalent to

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

Theorem.

Given two solutions (x_1, y_1) *and* (x_2, y_2) *in rational integers,*

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

define (x_3, y_3) *by writing*

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

Then (x_3, y_3) *is also a solution.*

Two solutions produce a third one

Proof.

From

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

we deduce

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

The product of the left hand sides

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

is $({x_1}^2 - d{y_1}^2)({x_2}^2 - d{y_2}^2) = \pm 1$, hence

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

which shows that (x_3, y_3) is also a solution. □

A multiplicative group

In the same way, given one solution (x, y), if we define (x', y') by writing

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

then

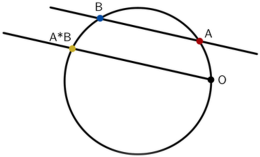
$$(x - y\sqrt{d})^{-1} = x' - y'\sqrt{d},$$

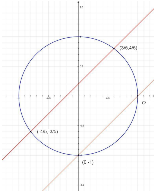
and it follows that (x', y') is again a solution.

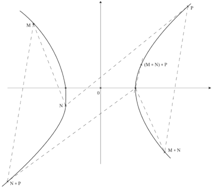
This means that the set of solutions in rational integers (positive or negative) is a *multiplicative group*. The trivial solution $(x, y) = (1, 0)$ is the unity of this group.

Group law on a conic

The curve $x^2 - Dy^2 = 1$ is a conic, and on a conic there is a group law which can be described geometrically. The fact that it is associative is proved by using Pascal's Theorem.







• Franz Lemmermeyer. *Conics – a poor man's elliptic curves.*
https://arxiv.org/pdf/math/0311306.pdf

• Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography*, Second Edition (Discrete Mathematics and Its Applications) **50**, Taylor & Francis Group, LLC (2008). https://doi.org/10.1201/9781420071474

• Peter Stevenhagen. *Complex elliptic curves* (2019).
http://www.rnta.eu/Montevideo2019/cimpa2019.pdf

The group of solutions $(x, y) \in \mathbb{Z} \times \mathbb{Z}$

Let G be the set of $(x, y) \in \mathbb{Z}^2$ satisfying $x^2 - dy^2 = \pm 1$. The bijection

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

endows G with a structure of multiplicative group.

The solution $(-1, 0)$ is a torsion element of order 2.

Infinitely many solutions

If there is a nontrivial solution (x_1, y_1) in positive integers, then there are infinitely many of them, which are obtained by writing

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

for $n = 1, 2, \ldots$.

We list the solutions by increasing values of $x + y\sqrt{d}$ (it amounts to the same to take the ordering given by x, or the one given by y).

Hence, assuming there is a non–trivial solution, it follows that there is a minimal solution > 1, which is called the *fundamental* solution.

Two important theorems

Let d be a positive integer which is not a square.

Theorem.
There is a non–trivial solution (x, y) *in positive integers to the equation* $x^2 - dy^2 = \pm 1$.

Hence there are infinitely many solutions in positive integers. And there is a smallest one, the fundamental solution (x_1, y_1). For any n in $\mathbb{Z}$ and any choice of the sign $\pm$, a solution (x, y) in rational integers is given by $\pm(x_1 + y_1\sqrt{d})^n = x + \sqrt{d}y$.

Theorem.
For any solution (x, y) *of the equation* $x^2 - dy^2 = \pm 1$, *there exists a rational integer* n *in* $\mathbb{Z}$ *and a sign* $\pm$, *such that* $x + \sqrt{d}y = \pm(x_1 + y_1\sqrt{d})^n$.

The group G has rank ≤ 1

Let φ denote the morphism

$$(x,y) \in G \longmapsto \bigl(\log |x+y\sqrt{d}|\ ,\ \log |x-y\sqrt{d}|\bigr) \in \mathbb{R}^2.$$

The kernel of φ is the torsion subgroup $\{(\pm 1, 0)\}$ of G. The image $\mathcal{G}$ of G is a discrete subgroup of the line $\{(t_1,t_2) \in \mathbb{R}^2\ ;\ t_1+t_2=0\}$. Hence there exists $u \in \mathcal{G}$ such that $\mathcal{G} = \mathbb{Z}u$.

Therefore the abelian group of all solutions in $\mathbb{Z} \times \mathbb{Z}$ has rank ≤ 1.

The existence of a solution other than $(\pm 1, 0)$ means that the rank of this group is 1.

$+1$ or -1 ?

• If the fundamental solution (x_1, y_1) of ${x_1}^2 - d{y_1}^2 = \pm 1$ produces the $+$ sign, then the equation $x^2 - dy^2 = -1$ has no solution.

• If the fundamental solution produces the $-$ sign, then the fundamental solution of the equation $x^2 - dy^2 = 1$ is (x_2, y_2) with $x_2 + y_2\sqrt{d} = (x_1 + y_1\sqrt{d})^2$, hence

$$x_2 = {x_1}^2 + d{y_1}^2, \qquad y_2 = 2x_1y_1.$$

The positive solutions of $x^2 - dy^2 = 1$ are the (x_n, y_n) with n even, the solutions of $x^2 - dy^2 = -1$ are obtained with n odd.

Algorithm for the fundamental solution

All the problem now is to find the fundamental solution.

Here is the idea. If x, y is a solution, then the equation $x^2 - dy^2 = \pm 1$, written as

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

shows that x/y is a good *rational approximation* to $\sqrt{d}$.

There is an algorithm for finding the *best* rational approximations of a real number : it is given by *continued fractions*.

The algorithm of continued fractions

Let $x \in \mathbb{R}$.

- Perform the Euclidean division of x by 1 :

$$x = \lfloor x \rfloor + \{x\} \quad \text{with } \lfloor x \rfloor \in \mathbb{Z} \text{ and } 0 \leq \{x\} < 1.$$

- In case x is an integer, this is the end of the algorithm. If x is not an integer, then $\{x\} \neq 0$ and we set $x_1 = 1/\{x\}$, so that

$$x = \lfloor x \rfloor + \frac{1}{x_1} \quad \text{with } \lfloor x \rfloor \in \mathbb{Z} \text{ and } x_1 > 1.$$

- In the case where x_1 is an integer, this is the end of the algorithm. If x_1 is not an integer, then we set $x_2 = 1/\{x_1\}$:

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

Continued fraction expansion

Set $a_0 = \lfloor x \rfloor$ and $a_i = \lfloor x_i \rfloor$ for $i \geq 1$.

- Then :

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

The algorithm stops after finitely many steps if and only if x is rational.

- We shall use the notation

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

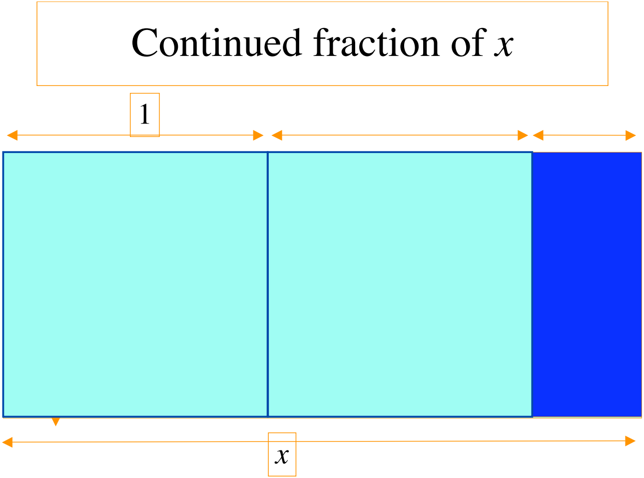
- Remark : if $a_k \geq 2$, then
$[a_0,\ a_1,\ a_2,\ a_3, \ldots, a_k] = [a_0,\ a_1,\ a_2,\ a_3, \ldots, a_k - 1, 1]$.

Continued fraction expansion : geometric point of view

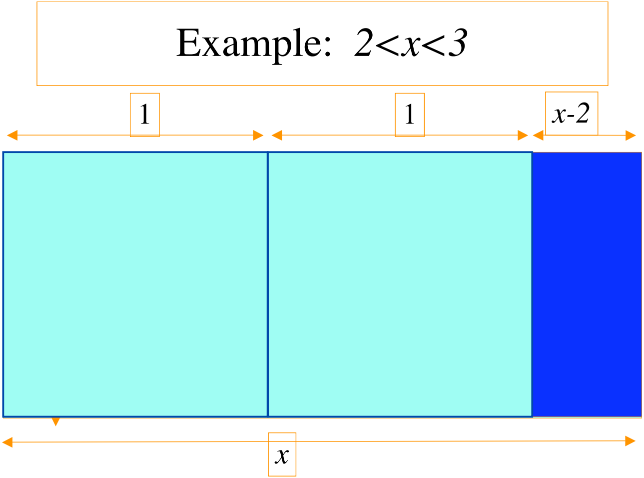
Start with a rectangle have side lengths 1 and x. The proportion is x.

Split it into $\lfloor x \rfloor$ squares with sides 1 and a smaller rectangle of sides $\{x\} = x - \lfloor x \rfloor$ and 1.

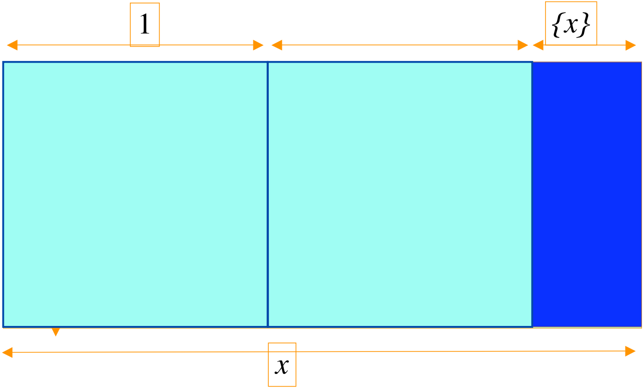
Rectangles with proportion x



Example : $2 < x < 3$



Number of squares : $a_0 = \lfloor x \rfloor$ with $x = \lfloor x \rfloor + \{x\}$



Continued fraction expansion : geometric point of view

Recall $x_1 = 1/\{x\}$

The small rectangle has side lengths in the proportion x_1.

Repeat the process : split the small rectangle into $\lfloor x_1 \rfloor$ squares and a third smaller rectangle, with sides in the proportion $x_2 = 1/\{x_1\}$.

This process produces the continued fraction expansion of x.

The sequence $a_0, a_1, \ldots$ is given by the number of squares at each step.

Example : the Golden Ratio

The Golden Ratio

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

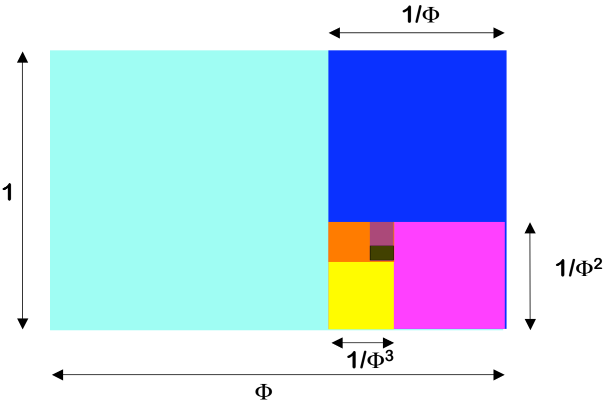
satisfies

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

Hence if we start with a rectangle having for proportion the Golden Ratio, at each step we get one square and a remaining smaller rectangle with sides in the same proportion.

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

Golden Rectangle



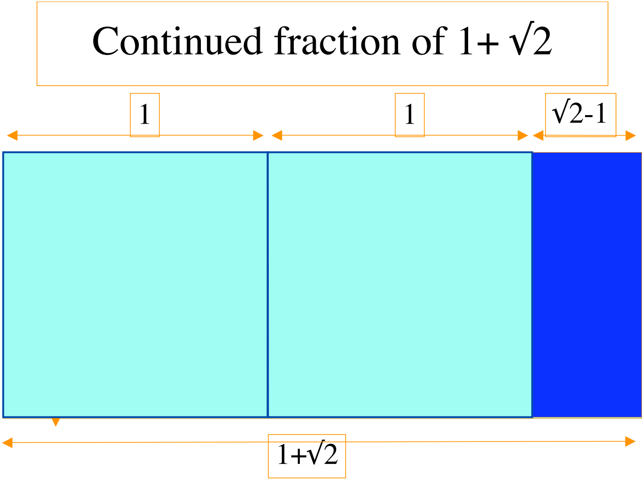
Rectangles with proportion $1+\sqrt{2}$

$$\sqrt{2} = 1.4142135623730950488016887242\ \ldots$$

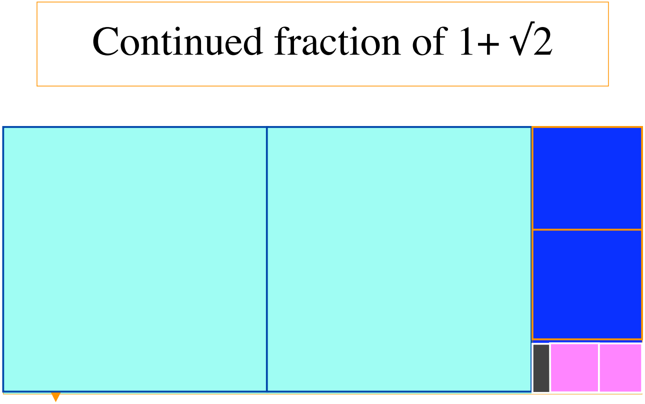
$$1+\sqrt{2} = 2 + \frac{1}{1+\sqrt{2}}$$

If we start with a rectangle having for proportion $1+\sqrt{2}$, at each step we get two squares and a remaining smaller rectangle with sides in the same proportion.

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



Rectangles with proportion $1 + \sqrt{2} = [2, 2, 2, 2 \ldots]$



Geometric proofs of irrationality

If we start with a rectangle having integer side lengths, at each step these squares have integral side lengths, smaller and smaller. Hence this process stops after finitely many steps.

Also for a rectangle with side lengths in a rational proportion, this process stops after finitely many steps (reduce to a common denominator and scale).

For instance Φ and $1+\sqrt{2}$ are irrational numbers, hence $\sqrt{5}$ and $\sqrt{2}$ also.

Continued fractions and rational Diophantine approximation

For

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

the sequence of rational numbers

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

produces rational approximations to x, and a classical result is that they are *the best possible ones* in terms of the quality of the approximation compared with the *size of the denominator.*

Continued fractions of a positive rational integer d

Recipe : let d be a positive integer which is not a square. Then the continued fraction of the number $\sqrt{d}$ is periodic.

If k is the smallest period length (that means that the length of any period is a positive integer multiple of k), this continued fraction can be written

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

with $a_k = 2a_0$ and $a_0 = \lfloor \sqrt{d} \rfloor$.

Further, $(a_1, a_2, \dots, a_{k-1})$ is a *palindrome*

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

Fact : the rational number given by the continued fraction $[a_0, a_1, \dots, a_{k-1}]$ is a good rational approximation to $\sqrt{d}$.

Parity of the length of the palindrome

If k is even, the fundamental solution of the equation $x^2 - dy^2 = 1$ is given by the fraction

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

In this case the equation $x^2 - dy^2 = -1$ has no solution.

Parity of the length of the palindrome

If k is odd, the fundamental solution (x_1, y_1) of the equation $x^2 - dy^2 = -1$ is given by the fraction

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

and the fundamental solution (x_2, y_2) of the equation $x^2 - dy^2 = 1$ by the fraction

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

Remark. In both cases where k is either even or odd, we obtain the sequence $(x_n, y_n)_{n\geq 1}$ of all solutions by repeating $n-1$ times $a_1, a_2, \ldots, a_k$ followed by $a_1, a_2, \ldots, a_{k-1}$.

The simplest Pell equation $x^2 - 2y^2 = \pm 1$

Euclid of Alexandria about 325 BC - about 265 BC ,
Elements, II § 10

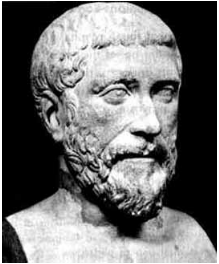
$$17^2 - 2 \cdot 12^2 = 289 - 2 \cdot 144 = 1.$$

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

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

Pythagorean triples

Pythagoras of Samos
about 569 BC - about 475 BC



Which are the right angle triangles with integer sides such that the two sides of the right angle are consecutive integers ?

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

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

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

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

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

Pell's equation $x^2 - 2y^2 = \pm 1$

- The fundamental solution of $x^2 - 2y^2 = -1$ is $(x_1, y_1) = (1, 1)$, with the continued fraction $[1]$.
The sequence of positive solutions $((x_{2n+1}, y_{2n+1}))_{n \geq 0}$ of $x^2 - 2y^2 = -1$ is given by $x_{2n+1} + y_{2n+1}\sqrt{2} = (1 + \sqrt{2})^{2n+1}$ with the continued fraction

$$\frac{x_{2n+1}}{y_{2n+1}} = [1, 2, 2, \ldots, 2]$$

a number of 2's which is $2n + 1$ (odd).
- The fundamental solution of $x^2 - 2y^2 = 1$ is $(x_2, y_2) = (3, 2)$, with the continued fraction $[1, 2] = 1 + \frac{1}{2} = \frac{3}{2}$.
The sequence of positive solutions $((x_{2n}, y_{2n}))_{n \geq 1}$ of $x^2 - 2y^2 = 1$ is given by $x_{2n} + y_{2n}\sqrt{2} = (1 + \sqrt{2})^{2n}$ with the continued fraction

$$\frac{x_{2n}}{y_{2n}} = [1, 2, 2, \ldots, 2]$$

a number of 2's which is $2n$ (even).

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

The continued fraction expansion of the number

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

is

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

because

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

The fundamental solution of $x^2 - 3y^2 = 1$ is $x = 2$, $y = 1$, corresponding to

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

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

The fundamental solution of $x^2 - 3y^2 = 1$ is $(x, y) = (2, 1)$:

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

There is no solution to the equation $x^2 - 3y^2 = -1$.
The period of the continued fraction

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

is $[1,\ 2]$ of even length 2.
Sequence of solutions of $x^2 - 3y^2 = 1$:

$$\frac{x_n}{y_n} = [1, 1, 2, 1, 2, \dots, 1, 2]$$

with n times the motive $1, 2$.

Small values of d

$$x^2 - 2y^2 = \pm 1,\ \sqrt{2} = [1, \overline{2}],\ k = 1,\ (x_1, y_1) = (1, 1),$$
$$1^2 - 2 \cdot 1^2 = -1.$$

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

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

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

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

Brahmagupta's Problem (628)

The continued fraction expansion of $\sqrt{92}$ is

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

The fundamental solution of the equation $x^2 - 92y^2 = 1$ is given by

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

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

Narayana's equation $x^2 - 103y^2 = 1$

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

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

Fundamental solution : $x = 227\,528$, $y = 22\,419$.

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

Equation of Bhaskhara II $x^2 - 61y^2 = \pm 1$

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

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

$29\ 718^2 = 883\ 159\ 524, \qquad 61 \cdot 3805^2 = 883\ 159\ 525$
is the fundamental solution of $x^2 - 61y^2 = -1$.

The fundamental solution of $x^2 - 61y^2 = 1$ is

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

Correspondence from Fermat to Brouncker

Pierre de Fermat — 1601 – 1665

Lord William Brouncker — 1620 – 1684

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

" *to make it not too difficult*"

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

Solutions respectively :

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

H.W. Lenstra Jr

H.W. Lenstra Jr

$$X^2 - 109Y^2 = 1$$

$$X = 158\,070\,671\,986\,249,$$

$$Y = 15\,140\,424\,455\,100$$

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

From 2020 to 2027

$$
\begin{aligned}
809^2 - 2020(18^2) &= 1 \quad \sqrt{2020} = [44, \overline{1, 16, 1, 88}] \\
45\ 495^2 - 2021(1012^2) &= 1 \quad \sqrt{2021} = [44, \overline{1, 21, 2, 21, 1, 88}] \\
1349\ 495^2 - 2022(30^2) &= 1 \quad \sqrt{2022} = [44, \overline{1, 28, 1, 88}] \\
2024^2 - 2023(45^2) &= 1 \quad \sqrt{2023} = [44, \overline{1, 43, 1, 88}] \\
45^2 - 2024 &= 1 \quad \sqrt{2024} = [44, \overline{1, 88}] \\
2025 &= 45^2 \\
40\ 051^2 - 2026(90^2) &= 1 \quad \sqrt{2026} = [45, \overline{90}] \\
2026^2 - 2027(45^2) &= 1 \quad \sqrt{2027} = [45, \overline{45, 90}].
\end{aligned}
$$

Back to Archimedes

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

Computation of the continued fraction of $\sqrt{410\,286\,423\,278\,424}$.

In 1867, C.F. Meyer performed the first 240 steps of the algorithm and then gave up.

The *length of the period* has now be computed : it is $203\,254$.

Solution by Amthor – Lenstra

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

Length of the period for $\sqrt{d'}$: 92.

Fundamental unit : $u = x' + y'\sqrt{d'}$

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

Fundamental solution of the Archimedes equation :

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

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

Size of the fundamental solution

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

Any method for solving the Brahmagupta–Fermat–Pell equation which requires to produce the digits of the fundamental solution has an exponential complexity.

Length L_d of the period :

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

Masser Problem 999

Find a quadratic polynomial $F(X,Y)$ over $\mathbb{Z}$ with coefficients of absolute value at most 999 (i.e. with at most three digits) such that the smallest integer solution of $F(X,Y)=0$ is as large as possible.

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

Smallest solution may be as large as $2^{H/5}$, and

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

Pell equation for 991 :

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

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

Arithmetic varieties

Let D be an integer which is not a square. The quadratic form $x^2 - Dy^2$ is anisotropic over $\mathbb{Q}$ (no non–trivial zero). Define $\mathcal{G} = \{(x, y) \in \mathbb{R}^2 \; ; \; x^2 - Dy^2 = 1\}$.

The map

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

is bijective : the inverse bijection is obtained by writing $u = 1/t$, $2x = t + u$, $2y\sqrt{D} = t - u$, so that $t = x + y\sqrt{D}$ and $u = x - y\sqrt{D}$.

Arithmetic varieties

By transport of structure, this endows

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

with a multiplicative group structure, isomorphic to $\mathbb{R}^\times$, for which

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

in an injective morphism of groups. Its image $G(\mathbb{R})$ is therefore isomorphic to $\mathbb{R}^\times$.

Arithmetic varieties

A matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ preserves the quadratic form $x^2 - Dy^2$ if and only if

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

which can be written

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

Hence the group of matrices of determinant 1 with coefficients in $\mathbb{Z}$ which preserve the quadratic form $x^2 - Dy^2$ is

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

Riemannian varieties with negative curvature

According to the works by Siegel, Harish–Chandra, Borel and Godement, the quotient of $G(\mathbb{R})$ by $G(\mathbb{Z})$ is compact. Hence $G(\mathbb{Z})$ is infinite (of rank 1 over $\mathbb{Z}$), which means that there are infinitely many integer solutions to the equation $a^2 - Dc^2 = 1$.

This is not a new proof of this result, but rather an interpretation and a generalization.

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://people.math.jussieu.fr/~bergeron/`

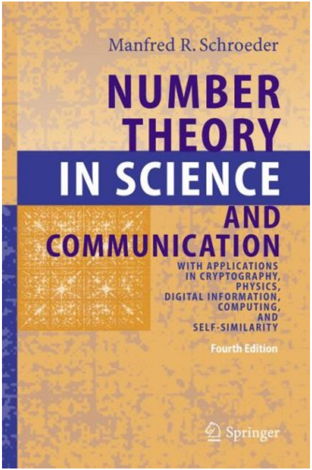
Substitutions in Christoffel's word

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

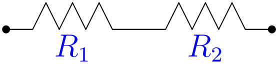
Number Theory in Science and communication

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.



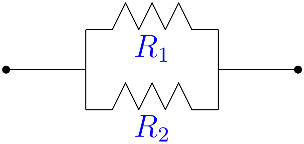
Electric networks

- The resistance of a network in series



is the sum $R_1 + R_2$.

- The resistance R of a network in parallel

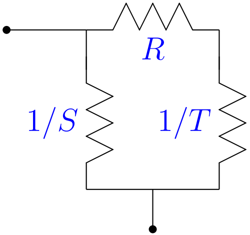


satisfies

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

Electric networks and continued fractions

The resistance U of the circuit

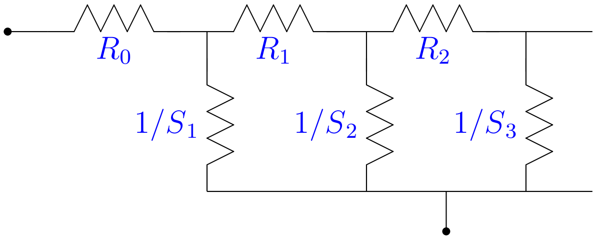


is given by

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

A circuit for a continued fraction expansion

- For the network



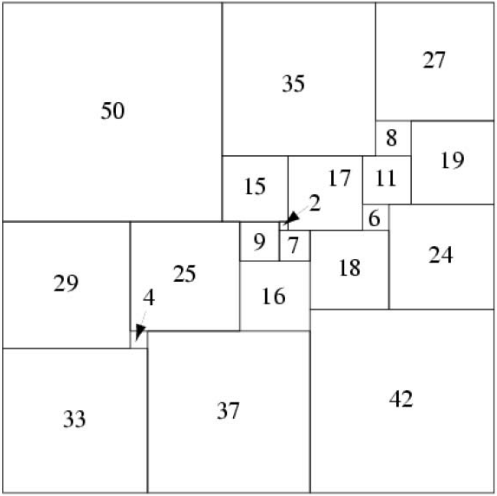
the resistance is given by a continued fraction expansion

$$R_0 + \cfrac{1}{S_1 + \cfrac{1}{R_1 + \cfrac{1}{S_2 + \cfrac{1}{\ddots}}}} := [R_0, S_1, R_1, S_2, R_2, \dots]$$

Decomposition of a square in squares

Electric networks and continued fractions have been used to find the first solution to the problem of decomposing an integer square into a disjoint union of integer squares, all of which are distinct.

Squaring the square



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.

On the Archimedes Cattle Problem and the Brahmagupta–Fermat–Pell Equation

Michel Waldschmidt

Professeur Émérite, Sorbonne Université
Institut de Mathématiques de Jussieu Paris Rive Gauche
http://www.imj-prg.fr/~michel.waldschmidt/