Mathematics Department, College of Science, Salahaddin University, Erbil (Kurdistan Iraq)

Topics in algebraic number theory and Diophantine approximation

Introduction to Diophantine Approximation (2)

On the Brahmagupta–Fermat–Pell equation

Michel Waldschmidt

Institut de Mathématiques de Jussieu — Paris VI
http://webusers.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

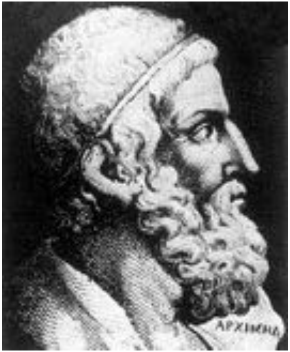
$$1\,151^2 - 92 \cdot 120^2 = 1, \qquad 1\,766\,319\,049^2 - 61 \cdot 226\,153\,980^2 = 1$$

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

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

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

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

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

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

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

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

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

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

Arithmetic constraints

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

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

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

Arithmetic constraints

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

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

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

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

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

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

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

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

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

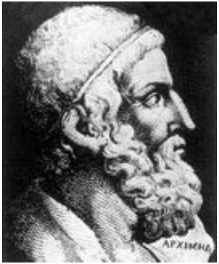
$$D=(2\cdot 4657)^2\cdot 4\,729\,494=410\,286\,423\,278\,424.$$

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)

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)

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)

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)

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)

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.

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.

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.

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.

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.

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.

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.

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*

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

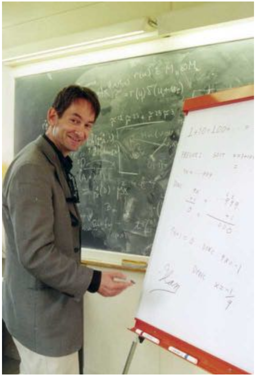
$10^{10^{10}}$ has $1 + 10^{10}$ decimal digits.

Ilan Vardi

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

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

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,
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.

Early results in India

Brahmagupta (598 – 670)
Brahmasphutasiddhanta : Composition method : *samasa* – Brahmagupta identity

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

Bhaskara II or Bhaskaracharya (1114 - 1185)
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://mathworld.wolfram.com/BrahmaguptasProblem.html
http://www-history.mcs.st-andrews.ac.uk/HistTopics/Pell.html

Early results in India

Brahmagupta (598 – 670)
Brahmasphutasiddhanta : Composition method : *samasa* – Brahmagupta identity

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

Bhaskara II or Bhaskaracharya (1114 - 1185)
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://mathworld.wolfram.com/BrahmaguptasProblem.html

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

History

John Pell : 1610–1685

Pierre de Fermat : 1601–1665
Letter to Frenicle in 1657

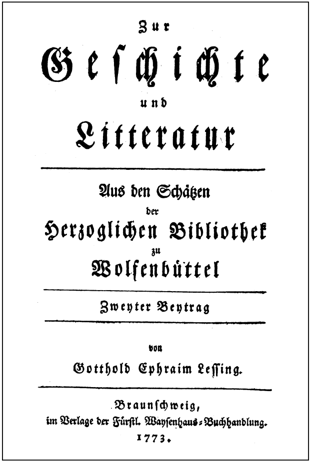
Lord William Brouncker : 1620–1684

Leonard Euler : 1707–1783
Book of algebra in 1770 + continued fractions

Joseph–Louis Lagrange : 1736–1813

1773 : Lagrange and Lessing


MÉLANGES
DE
PHILOSOPHIE ET DE MATHÉMATIQUE
DE LA
SOCIÉTÉ ROYALE
DE TURIN
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.

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.

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.

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.

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

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

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

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

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.

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. □

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. □

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 is the unity of this group.

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 is the unity of this group.

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 is the unity of this group.

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

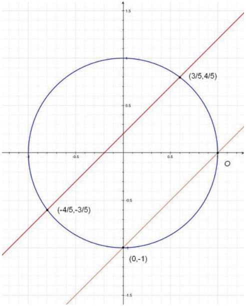
$$(x - y\sqrt{d})^{-1} = x' - y'\sqrt{d},$$

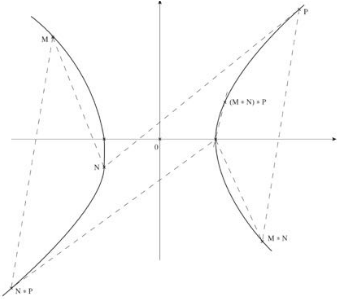
and it follows that (x', y') is again a solution.

This means that the set of solutions in rational integers (positive or negative) is a *multiplicative group*. The trivial solution 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.





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

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

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

endows G with a structure of multiplicative group.

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

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

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

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

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.

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.

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 $\mathbf{Z}$ and any choice of the sign $\pm$, a solution (x, y) in rational integers is given by $(x_1 + y_1\sqrt{d})^n = x + \sqrt{d}y$.

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

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 $\mathbf{Z}$ and any choice of the sign $\pm$, a solution (x, y) in rational integers is given by $(x_1 + y_1\sqrt{d})^n = x + \sqrt{d}y$.

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

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 $\mathbf{Z}$ and any choice of the sign $\pm$, a solution (x, y) in rational integers is given by $(x_1 + y_1\sqrt{d})^n = x + \sqrt{d}y$.

Theorem.
For any solution of the equation $x^2 - dy^2 = \pm 1$, there exists a rational integer n in $\mathbf{Z}$ 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

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

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 $\{(t_1, t_2) \in \mathbf{R}^2\ ;\ t_1 + t_2 = 0\}$. Hence there exists $u \in \mathcal{G}$ such that $\mathcal{G} = \mathbf{Z}u$.

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

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

The group G has rank ≤ 1

Let φ denote the morphism

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

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 $\{(t_1, t_2) \in \mathbf{R}^2\ ;\ t_1 + t_2 = 0\}$. Hence there exists $u \in \mathcal{G}$ such that $\mathcal{G} = \mathbf{Z}u$.

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

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

The group G has rank ≤ 1

Let φ denote the morphism

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

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 $\{(t_1,t_2) \in \mathbf{R}^2\ ;\ t_1+t_2=0\}$. Hence there exists $u \in \mathcal{G}$ such that $\mathcal{G} = \mathbf{Z}u$.

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

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

The group G has rank ≤ 1

Let φ denote the morphism

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

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 $\{(t_1, t_2) \in \mathbf{R}^2\ ;\ t_1 + t_2 = 0\}$. Hence there exists $u \in \mathcal{G}$ such that $\mathcal{G} = \mathbf{Z}u$.

Therefore the abelian group of all solutions in $\mathbf{Z} \times \mathbf{Z}$ 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 ${x_1}^2 - d{y_1}^2 = \pm 1$ produces the $+$ sign, then the equation $x^2 - dy^2 = -1$ has no solution.

- If the fundamental solution ${x_1}^2 - d{y_1}^2 = \pm 1$ 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 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.

$+1$ or -1 ?

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

- If the fundamental solution ${x_1}^2 - d{y_1}^2 = \pm 1$ 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 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.

$+1$ or -1 ?

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

- If the fundamental solution ${x_1}^2 - d{y_1}^2 = \pm 1$ 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 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*.

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*.

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*.

Continued fraction expansion : geometric point of view

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

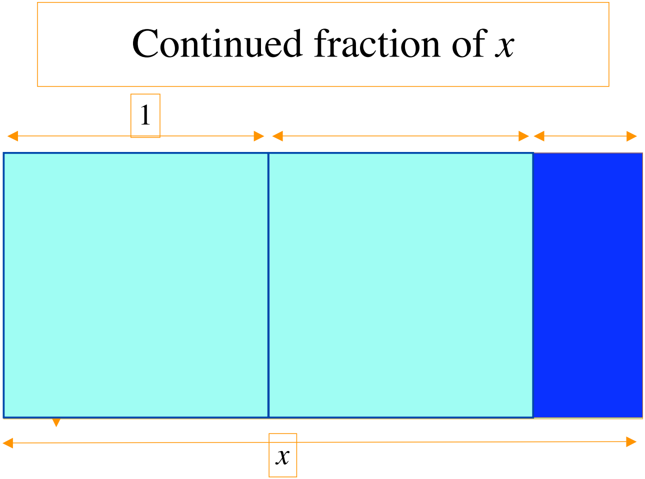
Split it into $\lfloor x \rfloor$ squares with sides 1 and a smaller rectangle of sides $\{x\} = x - \lfloor x \rfloor$ and 1.

Continued fraction expansion : geometric point of view

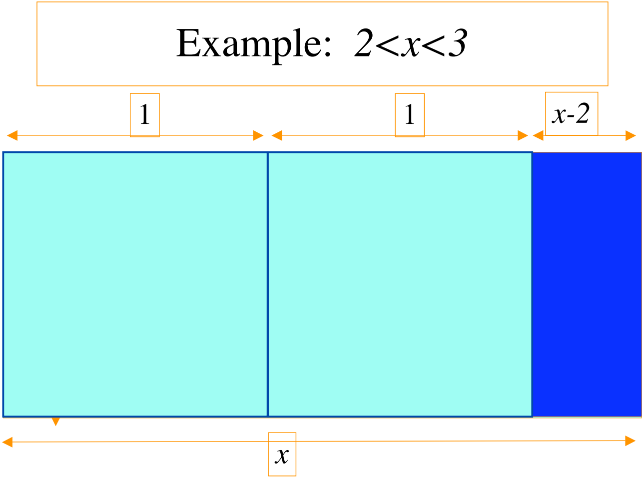
Start with a rectangle have side lengths 1 and x. The proportion is x.

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

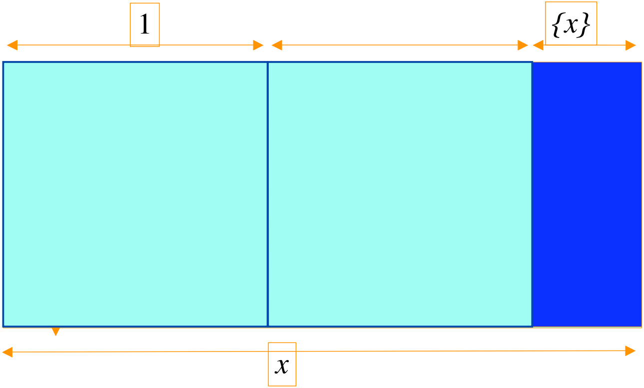
Rectangles with proportion x



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.

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

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.

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.

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

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*

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

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

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 $\sqrt{d}$.

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

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

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

Further, $(a_1, a_2, \ldots, a_{k-1})$ 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 $[a_0, a_1, \ldots, a_{k-1}]$ is a good rational approximation to $\sqrt{d}$.

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

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

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

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

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 $a_1, a_2, \dots, a_k$ followed by $a_1, a_2, \dots, a_{k-1}$.*

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

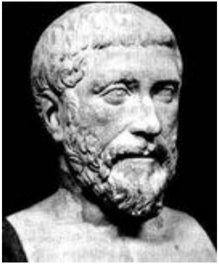
$17^2 - 2 \cdot 12^2 = 289 - 2 \cdot 144 = 1.$

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

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

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 ?

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

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

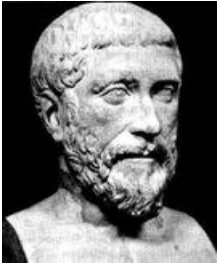
$$(2x+1)^2 - 2z^2 = -1$$

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

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

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 ?

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

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

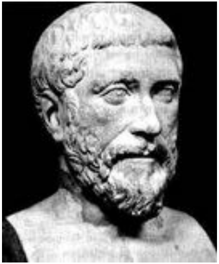
$$(2x + 1)^2 - 2z^2 = -1$$

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

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

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 ?

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

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

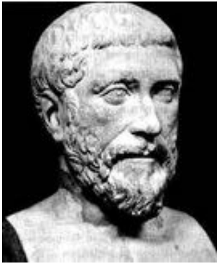
$$(2x+1)^2 - 2z^2 = -1$$

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

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

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 ?

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

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

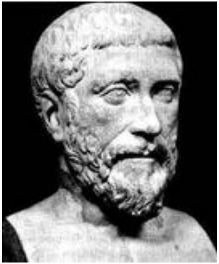
$$(2x+1)^2 - 2z^2 = -1$$

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

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

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 ?

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

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

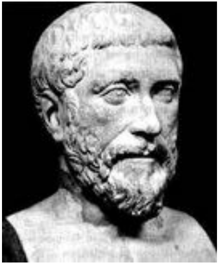
$$(2x+1)^2 - 2z^2 = -1$$

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

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

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 ?

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

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

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

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

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

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

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

satisfies

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

Hence the continued fraction expansion is periodic with period length 1 :

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

The fundamental solution of $x^2 - 2y^2 = -1$ is $x_1 = 1$, $y_1 = 1$

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

the continued fraction expansion of x_1/y_1 is $[1]$.

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

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

satisfies

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

Hence the continued fraction expansion is periodic with period length 1 :

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

The fundamental solution of $x^2 - 2y^2 = -1$ is $x_1 = 1$, $y_1 = 1$

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

the continued fraction expansion of x_1/y_1 is $[1]$.

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

$$\sqrt{2} = 1,41421356237309504880168872 42 \ \dots$$

satisfies

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

Hence the continued fraction expansion is periodic with period length 1 :

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

The fundamental solution of $x^2 - 2y^2 = -1$ is $x_1 = 1$, $y_1 = 1$

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

the continued fraction expansion of x_1/y_1 is $[1]$.

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

The fundamental solution of

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

is $x = 3$, $y = 2$, given by

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

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

The continued fraction expansion of the number

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

is

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

because

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

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

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

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

The continued fraction expansion of the number

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

is

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

because

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

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

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

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

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.

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

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.

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

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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2015 and 2016

For $d = 2015$,

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

period length 4, fundamental solution

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

For $d = 2016$,

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

period length 4, fundamental solution

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

2015 and 2016

For $d = 2015$,

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

period length 4, fundamental solution

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

For $d = 2016$,

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

period length 4, fundamental solution

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

2015 and 2016

For $d = 2015$,

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

period length 4, fundamental solution

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

For $d = 2016$,

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

period length 4, fundamental solution

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

2015 and 2016

For $d = 2015$,

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

period length 4, fundamental solution

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

For $d = 2016$,

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

period length 4, fundamental solution

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

2015 and 2016

For $d = 2015$,

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

period length 4, fundamental solution

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

For $d = 2016$,

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

period length 4, fundamental solution

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

2015 and 2016

For $d = 2015$,

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

period length 4, fundamental solution

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

For $d = 2016$,

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

period length 4, fundamental solution

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

wims : WWW Interactive Multipurpose Server

Exercise : for 2017, compute the period length and the number of digits of the fundamental solution.

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

The continued fraction is computed by PARI version 2.2.1.

http://wims.unice.fr/wims/wims.cgi?session=F

Contfrac

Développement en fraction continue de n = sqrt(2017) :

44.9110231457712394878062089365972338782374214688669731766907614027262259928013395335655867933632416255007839800404888650447040511234191204884547315225315691652629071598683088864471092576548485494997

44 + 1/1+ 1/10+ 1/4+ 1/5+ 1/2+ 1/1+ 1/2+ 1/2+ 1/2+ 1/3+ 1/3+ 1/29+ 1/1+ 1/1+ 1/1+ 1/3+ 1/12+ 1/1+ 1/1+ 1/3+ 1/1+ 1/3+ 1/7+ 1/1+ 1/9+ 1/9+ 1/1+ 1/7+ 1/3+ 1/1+ 1/3+ 1/1+ 1/1+ 1/12+ 1/3+ 1/1+ 1/1+ 1/1+ 1/29+ 1/3+ 1/3+ 1/2+ 1/2+ 1/2+ 1/1
1/4+ 1/10+ 1/1+ 1/88+ 1/1+ 1/10+ 1/4+ 1/5+ 1/2+ 1/1+ 1/2+ 1/2+ 1/2+ 1/3+ 1/3+ 1/29+ 1/1+ 1/1+ 1/1+ 1/3+ 1/12+ 1/1+ 1/1+ 1/3+ 1/1+ 1/3+ 1/7+ 1/1+ 1/9+ 1/9+ 1/1+ 1/7+ 1/3+ 1/1+ 1/3+ 1/1+ 1/1+ 1/12+ 1/3+ 1/1+ 1/1+ 1/1+ 1/29+ 1/3+ 1/3+ 1
1/1+ 1/2+ 1/5+ 1/4+ 1/10+ 1/1+ 1/88+ 1/1+ 1/10+ 1/4+ 1/5+ 1/2+ 1/1+ 1/2+ 1/2+ 1/2+ 1/3+ 1/3+ 1/29+ 1/1+ 1/1+ 1/1+ 1/3+ 1/12+ 1/1+ 1/1+ 1/3+ 1/1+ 1/3+ 1/7+ 1/1+ 1/9+ 1/9+ 1/1+ 1/7+ 1/3+ 1/1+ 1/3+ 1/1+ 1/1+ 1/12+ 1/3+ 1/1+ 1/1+ 1/1+ 1/
1/2+ 1/2+ 1/2+ 1/1+ 1/2+ 1/5+ 1/4+ 1/10+ 1/1+ 1/88+ 1/1+ 1/10+ 1/4+ 1/5+ 1/2+ 1/1+ 1/2+ 1/2+ 1/2+ 1/3+ 1/3+ 1/29+ 1/1+ 1/1+ 1/1+ 1/3+ 1/12+ 1/1+ 1/1+ 1/3+ 1/1+ 1/3+ 1/7+ 1/1+ 1/9+ 1/9+ 1/1+ 1/7+ 1/3+ 1/1+ 1/3+ 1/1+ 1/1+ 1/12+ 1/3+ 1/
1/29+ 1/3+ 1/3+ 1/2+ 1/2+ 1/2+ 1/1+ 1/2+ . . .

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

Mode de présentation de la fraction continue :

$n_1 + {}^1/_{n_2+} {}^1/_{n_3+} {}^1/_{n_4+} {}^1/_{n_5+} \dots$ = $$ n_1+{\strut 1\over\displaystyle n_2+ {\strut 1\over\displaystyle n_3+ {\strut 1\over\displaystyle n_4+ {\strut 1\over\displaystyle n_5+\cdots}}}} $$

Développer un autre nombre.

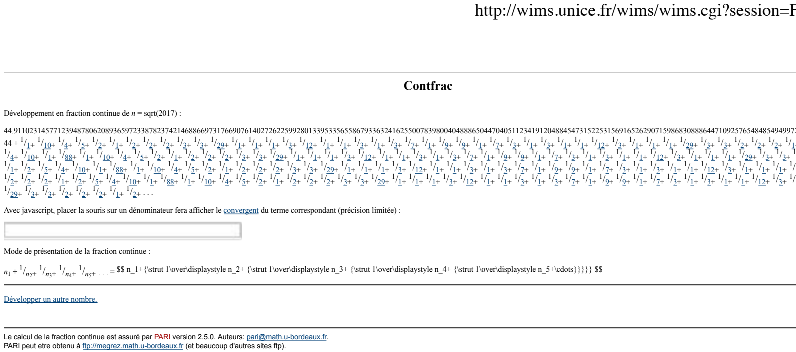
Le calcul de la fraction continue est assuré par PARI version 2.5.0. Auteurs: pari@math.u-bordeaux.fr.
PARI peut etre obtenu à ftp://megrez.math.u-bordeaux.fr (et beaucoup d'autres sites ftp).

wims : WWW Interactive Multipurpose Server

Exercise : for 2017, compute the period length and the number of digits of the fundamental solution.

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

The continued fraction is computed by PARI version 2.2.1.



http://wims.unice.fr/wims/wims.cgi?session=F

Contfrac

Développement en fraction continue de n = sqrt(2017) :

44.91102314577123948780620893659723387823742146886697317669076140272622599280133953356558679336324162550078398004048886504470405112341912048845473152253156916526290715986830888644710925765484854949997

44 + 1/1+ 1/10+ 1/4+ 1/5+ 1/2+ 1/1+ 1/2+ 1/2+ 1/2+ 1/3+ 1/3+ 1/29+ 1/1+ 1/1+ 1/1+ 1/3+ 1/12+ 1/1+ 1/1+ 1/3+ 1/1+ 1/3+ 1/7+ 1/1+ 1/9+ 1/9+ 1/1+ 1/7+ 1/3+ 1/1+ 1/3+ 1/1+ 1/1+ 1/12+ 1/3+ 1/1+ 1/1+ 1/1+ 1/29+ 1/3+ 1/3+ 1/2+ 1/2+ 1/2+ 1/1
1/4+ 1/10+ 1/1+ 1/88+ 1/1+ 1/10+ 1/4+ 1/5+ 1/2+ 1/1+ 1/2+ 1/2+ 1/2+ 1/3+ 1/3+ 1/29+ 1/1+ 1/1+ 1/1+ 1/3+ 1/12+ 1/1+ 1/1+ 1/3+ 1/1+ 1/3+ 1/7+ 1/1+ 1/9+ 1/9+ 1/1+ 1/7+ 1/3+ 1/1+ 1/3+ 1/1+ 1/1+ 1/12+ 1/3+ 1/1+ 1/1+ 1/1+ 1/29+ 1/3+ 1/3+
1/1+ 1/2+ 1/5+ 1/4+ 1/10+ 1/1+ 1/88+ 1/1+ 1/10+ 1/4+ 1/5+ 1/2+ 1/1+ 1/2+ 1/2+ 1/2+ 1/3+ 1/3+ 1/29+ 1/1+ 1/1+ 1/1+ 1/3+ 1/12+ 1/1+ 1/1+ 1/3+ 1/1+ 1/3+ 1/7+ 1/1+ 1/9+ 1/9+ 1/1+ 1/7+ 1/3+ 1/1+ 1/3+ 1/1+ 1/1+ 1/12+ 1/3+ 1/1+ 1/1+ 1/1+
1/2+ 1/2+ 1/2+ 1/1+ 1/2+ 1/5+ 1/4+ 1/10+ 1/1+ 1/88+ 1/1+ 1/10+ 1/4+ 1/5+ 1/2+ 1/1+ 1/2+ 1/2+ 1/2+ 1/3+ 1/3+ 1/29+ 1/1+ 1/1+ 1/1+ 1/3+ 1/12+ 1/1+ 1/1+ 1/3+ 1/1+ 1/3+ 1/7+ 1/1+ 1/9+ 1/9+ 1/1+ 1/7+ 1/3+ 1/1+ 1/3+ 1/1+ 1/1+ 1/12+ 1/3+
1/29+ 1/3+ 1/3+ 1/2+ 1/2+ 1/2+ 1/1+ 1/2+ . . .

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

Mode de présentation de la fraction continue :

$n_1 + {}^1/_{n_2+}\ {}^1/_{n_3+}\ {}^1/_{n_4+}\ {}^1/_{n_5+} \dots$ = `$$ n_1+{\strut 1\over\displaystyle n_2+ {\strut 1\over\displaystyle n_3+ {\strut 1\over\displaystyle n_4+ {\strut 1\over\displaystyle n_5+\cdots}}}} $$`

Développer un autre nombre.

Le calcul de la fraction continue est assuré par PARI version 2.5.0. Auteurs: pari@math.u-bordeaux.fr.
PARI peut etre obtenu à ftp://megrez.math.u-bordeaux.fr (et beaucoup d'autres sites ftp).

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 $203\,254$.

Back to Archimedes

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

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 $203\,254$.

Back to Archimedes

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

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 $203\,254$.

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

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

Fundamental solution of the Archimedes equation :

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

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

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

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

Fundamental solution of the Archimedes equation :

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

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

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

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

Fundamental solution of the Archimedes equation :

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

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

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

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

Fundamental solution of the Archimedes equation :

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

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

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

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

Fundamental solution of the Archimedes equation :

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

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

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

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

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 :

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

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 :

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

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 $\mathbf{Z}$ 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 :

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

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

Masser Problem 999

Find a quadratic polynomial $F(X, Y)$ over $\mathbf{Z}$ 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 :

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

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

Masser Problem 999

Find a quadratic polynomial $F(X,Y)$ over $\mathbf{Z}$ 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 :

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

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

Masser Problem 999

Find a quadratic polynomial $F(X,Y)$ over $\mathbf{Z}$ 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 :

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

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

Masser Problem 999

Find a quadratic polynomial $F(X, Y)$ over $\mathbf{Z}$ 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 $\mathbf{Q}$ (no non–trivial zero). Define $\mathcal{G} = \{(x, y) \in \mathbf{R}^2 \; ; \; x^2 - Dy^2 = 1\}$.

The map

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

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

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

The map

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

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

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

The map

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

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

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

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

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

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

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 $\mathbf{Z}$ which preserve the quadratic form $x^2 - Dy^2$ is

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

Riemannian varieties with negative curvature

According to the works by Siegel, Harish–Chandra, Borel and Godement, the quotient of $G(\mathbf{R})$ by $G(\mathbf{Z})$ is compact. Hence $G(\mathbf{Z})$ is infinite (of rank 1 over $\mathbf{Z}$), 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/`

Riemannian varieties with negative curvature

According to the works by Siegel, Harish–Chandra, Borel and Godement, the quotient of $G(\mathbf{R})$ by $G(\mathbf{Z})$ is compact. Hence $G(\mathbf{Z})$ is infinite (of rank 1 over $\mathbf{Z}$), 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/

Riemannian varieties with negative curvature

According to the works by Siegel, Harish–Chandra, Borel and Godement, the quotient of $G(\mathbf{R})$ by $G(\mathbf{Z})$ is compact. Hence $G(\mathbf{Z})$ is infinite (of rank 1 over $\mathbf{Z}$), 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

Rational approximations to a real numbers

If x is a rational number, there is a constant $c > 0$ such that for any $p/q \in \mathbf{Q}$ with $p/q \neq x$, we have $|x - p/q| \geq c/q$.

Proof : write $x = a/b$ and set $c = 1/b$.

If x is a real irrational number, there are infinitely many $p/q \in \mathbf{Q}$ with $|x - p/q| < 1/q^2$.

The best rational approximations p/q are given by the algorithm of continued fraction.

With a single real number x, it amounts to the same to investigate $|x - \frac{p}{q}|$ or $|qx - p|$ for p, q in $\mathbf{Z}$, $q > 0$.

Rational approximations to a real numbers

If x is a rational number, there is a constant $c > 0$ such that for any $p/q \in \mathbf{Q}$ with $p/q \neq x$, we have $|x - p/q| \geq c/q$.

Proof : write $x = a/b$ and set $c = 1/b$.

If x is a real irrational number, there are infinitely many $p/q \in \mathbf{Q}$ with $|x - p/q| < 1/q^2$.

The best rational approximations p/q are given by the algorithm of continued fraction.

With a single real number x, it amounts to the same to investigate $|x - \frac{p}{q}|$ or $|qx - p|$ for p, q in $\mathbf{Z}$, $q > 0$.

Rational approximation to a single number

Continued fractions (Leonhard Euler)

Farey dissection (Sir John Farey)

Dirichlet's Box Principle (Gustav Lejeune – Dirichlet)

Geometry of numbers (Hermann Minkowski)

Euler

(1707 – 1783)

Farey

(1766 – 1826)

Dirichlet

(1805 – 1859)

Minkowski

(1864–1909)

Continued fractions : the convergents

Given rational integers $a_0, a_1, \ldots, a_n$ with $a_i \geq 1$ for $i \geq 1$, the finite continued fraction

$$[a_0,\ a_1,\ a_2,\ a_3, \ldots, a_n]$$

can be written

$$\frac{P_n(a_0, a_1, \ldots, a_n)}{Q_n(a_1, a_2, \ldots, a_n)}$$

where P_n and Q_n are polynomials with integer coefficients. We wish to write these polynomials explicitly.

Continued fractions : the convergents

Let $\mathbf{F}$ be a field, $Z_0, Z_1, \ldots$ variables. We will define polynomials P_n and Q_n in $\mathbf{F}[Z_0, \ldots, Z_n]$ and $\mathbf{F}[Z_1, \ldots, Z_n]$ respectively such that

$$[Z_0, Z_1, \ldots, Z_n] = \frac{P_n}{Q_n}.$$

Here are the first values :

$$P_0 = Z_0, \quad Q_0 = 1, \quad \frac{P_0}{Q_0} = Z_0;$$

$$P_1 = Z_0 Z_1 + 1, \quad Q_1 = Z_1, \quad \frac{P_1}{Q_1} = Z_0 + \frac{1}{Z_1};$$

$$P_2 = Z_0 Z_1 Z_2 + Z_2 + Z_0, \quad Q_2 = Z_1 Z_2 + 1, \quad \frac{P_2}{Q_2} = Z_0 + \frac{1}{Z_1 + \frac{1}{Z_2}}.$$

Continued fractions : the convergents

Let $\mathbf{F}$ be a field, $Z_0, Z_1, \ldots$ variables. We will define polynomials P_n and Q_n in $\mathbf{F}[Z_0, \ldots, Z_n]$ and $\mathbf{F}[Z_1, \ldots, Z_n]$ respectively such that

$$[Z_0, Z_1, \ldots, Z_n] = \frac{P_n}{Q_n}.$$

Here are the first values :

$$P_0 = Z_0, \quad Q_0 = 1, \quad \frac{P_0}{Q_0} = Z_0;$$

$$P_1 = Z_0 Z_1 + 1, \quad Q_1 = Z_1, \quad \frac{P_1}{Q_1} = Z_0 + \frac{1}{Z_1};$$

$$P_2 = Z_0 Z_1 Z_2 + Z_2 + Z_0, \quad Q_2 = Z_1 Z_2 + 1, \quad \frac{P_2}{Q_2} = Z_0 + \cfrac{1}{Z_1 + \cfrac{1}{Z_2}}.$$

Continued fractions : the convergents

Let $\mathbf{F}$ be a field, $Z_0, Z_1, \ldots$ variables. We will define polynomials P_n and Q_n in $\mathbf{F}[Z_0, \ldots, Z_n]$ and $\mathbf{F}[Z_1, \ldots, Z_n]$ respectively such that

$$[Z_0, Z_1, \ldots, Z_n] = \frac{P_n}{Q_n}.$$

Here are the first values :

$$P_0 = Z_0, \quad Q_0 = 1, \quad \frac{P_0}{Q_0} = Z_0;$$

$$P_1 = Z_0 Z_1 + 1, \quad Q_1 = Z_1, \quad \frac{P_1}{Q_1} = Z_0 + \frac{1}{Z_1};$$

$$P_2 = Z_0 Z_1 Z_2 + Z_2 + Z_0, \quad Q_2 = Z_1 Z_2 + 1, \quad \frac{P_2}{Q_2} = Z_0 + \frac{1}{Z_1 + \frac{1}{Z_2}}.$$

Continued fractions : the convergents

Let $\mathbf{F}$ be a field, $Z_0, Z_1, \ldots$ variables. We will define polynomials P_n and Q_n in $\mathbf{F}[Z_0, \ldots, Z_n]$ and $\mathbf{F}[Z_1, \ldots, Z_n]$ respectively such that

$$[Z_0, Z_1, \ldots, Z_n] = \frac{P_n}{Q_n}.$$

Here are the first values :

$$P_0 = Z_0, \quad Q_0 = 1, \quad \frac{P_0}{Q_0} = Z_0;$$

$$P_1 = Z_0 Z_1 + 1, \quad Q_1 = Z_1, \quad \frac{P_1}{Q_1} = Z_0 + \frac{1}{Z_1};$$

$$P_2 = Z_0 Z_1 Z_2 + Z_2 + Z_0, \quad Q_2 = Z_1 Z_2 + 1, \quad \frac{P_2}{Q_2} = Z_0 + \frac{1}{Z_1 + \frac{1}{Z_2}}.$$

Continued fractions : the convergents

$$P_3 = Z_0Z_1Z_2Z_3 + Z_2Z_3 + Z_0Z_3 + Z_0Z_1 + 1,$$

$$Q_3 = Z_1Z_2Z_3 + Z_3 + Z_1,$$

$$\frac{P_3}{Q_3} = Z_0 + \cfrac{1}{Z_1 + \cfrac{1}{Z_2 + \cfrac{1}{Z_3}}}.$$

$$P_2 = Z_2P_1 + P_0, \quad Q_2 = Z_2Q_1 + Q_0.$$

$$P_3 = Z_3P_2 + P_1, \quad Q_3 = Z_3Q_2 + Q_1.$$

Continued fractions : the convergents

$$P_3 = Z_0 Z_1 Z_2 Z_3 + Z_2 Z_3 + Z_0 Z_3 + Z_0 Z_1 + 1,$$

$$Q_3 = Z_1 Z_2 Z_3 + Z_3 + Z_1,$$

$$\frac{P_3}{Q_3} = Z_0 + \cfrac{1}{Z_1 + \cfrac{1}{Z_2 + \cfrac{1}{Z_3}}}.$$

$$P_2 = Z_2 P_1 + P_0, \quad Q_2 = Z_2 Q_1 + Q_0.$$

$$P_3 = Z_3 P_2 + P_1, \quad Q_3 = Z_3 Q_2 + Q_1.$$

Continued fractions : the convergents

$$P_3 = Z_0Z_1Z_2Z_3 + Z_2Z_3 + Z_0Z_3 + Z_0Z_1 + 1,$$

$$Q_3 = Z_1Z_2Z_3 + Z_3 + Z_1,$$

$$\frac{P_3}{Q_3} = Z_0 + \cfrac{1}{Z_1 + \cfrac{1}{Z_2 + \cfrac{1}{Z_3}}}.$$

$$P_2 = Z_2P_1 + P_0, \quad Q_2 = Z_2Q_1 + Q_0.$$

$$P_3 = Z_3P_2 + P_1, \quad Q_3 = Z_3Q_2 + Q_1.$$

Continued fractions : the convergents

$$P_3 = Z_0 Z_1 Z_2 Z_3 + Z_2 Z_3 + Z_0 Z_3 + Z_0 Z_1 + 1,$$

$$Q_3 = Z_1 Z_2 Z_3 + Z_3 + Z_1,$$

$$\frac{P_3}{Q_3} = Z_0 + \cfrac{1}{Z_1 + \cfrac{1}{Z_2 + \cfrac{1}{Z_3}}}.$$

$$P_2 = Z_2 P_1 + P_0, \quad Q_2 = Z_2 Q_1 + Q_0.$$

$$P_3 = Z_3 P_2 + P_1, \quad Q_3 = Z_3 Q_2 + Q_1.$$

Continued fractions : the convergents

For $n = 2$ and $n = 3$, we observe that

$$P_n = Z_n P_{n-1} + P_{n-2}, \quad Q_n = Z_n Q_{n-1} + Q_{n-2}.$$

This will be our definition of P_n and Q_n.

In matrix form, it is

$$\begin{pmatrix} P_n \\ Q_n \end{pmatrix} = \begin{pmatrix} P_{n-1} & P_{n-2} \\ Q_{n-1} & Q_{n-2} \end{pmatrix} \begin{pmatrix} Z_n \\ 1 \end{pmatrix}.$$

Continued fractions : the convergents

For $n = 2$ and $n = 3$, we observe that

$$P_n = Z_n P_{n-1} + P_{n-2}, \quad Q_n = Z_n Q_{n-1} + Q_{n-2}.$$

This will be our definition of P_n and Q_n.

In matrix form, it is

$$\begin{pmatrix} P_n \\ Q_n \end{pmatrix} = \begin{pmatrix} P_{n-1} & P_{n-2} \\ Q_{n-1} & Q_{n-2} \end{pmatrix} \begin{pmatrix} Z_n \\ 1 \end{pmatrix}.$$

Definition of P_n and Q_n

With 2×2 matrices :

$$\begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} = \begin{pmatrix} P_{n-1} & P_{n-2} \\ Q_{n-1} & Q_{n-2} \end{pmatrix} \begin{pmatrix} Z_n & 1 \\ 1 & 0 \end{pmatrix}.$$

Hence :

$$\begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} = \begin{pmatrix} Z_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} Z_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} Z_n & 1 \\ 1 & 0 \end{pmatrix}.$$

Definition of P_n and Q_n

With 2×2 matrices :

$$\begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} = \begin{pmatrix} P_{n-1} & P_{n-2} \\ Q_{n-1} & Q_{n-2} \end{pmatrix} \begin{pmatrix} Z_n & 1 \\ 1 & 0 \end{pmatrix}.$$

Hence :

$$\begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} = \begin{pmatrix} Z_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} Z_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} Z_n & 1 \\ 1 & 0 \end{pmatrix}.$$

Continued fractions : definition of P_n and Q_n

$$\begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} = \begin{pmatrix} Z_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} Z_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} Z_n & 1 \\ 1 & 0 \end{pmatrix} \quad \text{for } n \geq -1.$$

In particular

$$\begin{pmatrix} P_{-1} & P_{-2} \\ Q_{-1} & Q_{-2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

One checks $[Z_0, Z_1, \ldots, Z_n] = P_n/Q_n$ for all $n \geq 0$.

Continued fractions : definition of P_n and Q_n

$$\begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} = \begin{pmatrix} Z_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} Z_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} Z_n & 1 \\ 1 & 0 \end{pmatrix} \quad \text{for } n \geq -1.$$

In particular

$$\begin{pmatrix} P_{-1} & P_{-2} \\ Q_{-1} & Q_{-2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

One checks $[Z_0, Z_1, \ldots, Z_n] = P_n/Q_n$ for all $n \geq 0$.

Continued fractions : definition of P_n and Q_n

$$\begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} = \begin{pmatrix} Z_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} Z_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} Z_n & 1 \\ 1 & 0 \end{pmatrix} \quad \text{for } n \geq -1.$$

In particular

$$\begin{pmatrix} P_{-1} & P_{-2} \\ Q_{-1} & Q_{-2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

One checks $[Z_0, Z_1, \ldots, Z_n] = P_n/Q_n$ for all $n \geq 0$.

Simple continued fraction of a real number

For

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

we have

$$x = \frac{p_n}{q_n}$$

with

$$p_n = P_n(a_0, a_1, \ldots, a_n) \quad \text{and} \quad q_n = Q_n(a_1, \ldots, a_n).$$

Simple continued fraction of a real number

For

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

the rational numbers in the sequence

$$\frac{p_n}{q_n} = [a_0,\ a_1,\ a_2, \ldots, a_n] \qquad (k = 1, 2, \ldots)$$

give rational approximations for x which are the best ones when comparing the quality of the approximation and the size of the denominator.

$a_0, a_1, a_2, \ldots$ are the *partial quotients*,
p_n/q_n $(n \geq 0)$ are the *convergents*.
$x_n = [a_n, a_{n+1}, \ldots]$ $(n \geq 0)$ are the *complete quotients*.
Hence

$$x = [a_0, a_1, \ldots, a_{n-1}, x_n] = \frac{x_n p_{n-1} + p_{n-2}}{x_n q_{n-1} + q_{n-2}}.$$

Simple continued fraction of a real number

For

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

the rational numbers in the sequence

$$\frac{p_n}{q_n} = [a_0,\ a_1,\ a_2, \dots, a_n] \qquad (k = 1, 2, \dots)$$

give rational approximations for x which are the best ones when comparing the quality of the approximation and the size of the denominator.

$a_0, a_1, a_2, \dots$ are the *partial quotients*,

p_n/q_n $(n \geq 0)$ are the *convergents*.

$x_n = [a_n, a_{n+1}, \dots]$ $(n \geq 0)$ are the *complete quotients*.

Hence

$$x = [a_0, a_1, \dots, a_{n-1}, x_n] = \frac{x_n p_{n-1} + p_{n-2}}{x_n q_{n-1} + q_{n-2}}.$$

Simple continued fraction of a real number

For

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

the rational numbers in the sequence

$$\frac{p_n}{q_n} = [a_0,\ a_1,\ a_2, \ldots, a_n] \qquad (k = 1, 2, \ldots)$$

give rational approximations for x which are the best ones when comparing the quality of the approximation and the size of the denominator.

$a_0, a_1, a_2, \ldots$ are the *partial quotients*,

p_n/q_n $(n \geq 0)$ are the *convergents*.

$x_n = [a_n, a_{n+1}, \ldots]$ $(n \geq 0)$ are the *complete quotients*.

Hence

$$x = [a_0, a_1, \ldots, a_{n-1}, x_n] = \frac{x_n p_{n-1} + p_{n-2}}{x_n q_{n-1} + q_{n-2}}.$$

Continued fractions and rational approximation

From

$$q_n = a_n q_{n-1} + q_{n-2} \quad \text{and} \quad q_n x - p_n = \frac{(-1)^n}{a_{n+1} q_n + q_{n-1}}$$

one deduces the inequalities

$$a_n q_{n-1} \le q_n \le (a_n + 1) q_{n-1}$$

and

$$\frac{1}{(a_{n+1}+2)q_n} < \frac{1}{q_{n+1}+q_n} < |q_n x - p_n| < \frac{1}{q_{n+1}} < \frac{1}{a_{n+1} q_n}.$$

Convergents are the best rational approximations

Let p_n/q_n be the n–th convergent of the continued fraction expansion of an irrational number x.

Theorem. Let a/b be any rational number such that $1 \leq b \leq q_n$. Then :

$$|q_n x - p_n| \leq |bx - a|$$

with equality if and only if $(a, b) = (p_n, q_n)$.

Corollary. For $1 \leq b \leq q_n$ we have

$$\left| x - \frac{p_n}{q_n} \right| \leq \left| x - \frac{a}{b} \right|$$

with equality if and only if $(a, b) = (p_n, q_n)$.

Convergents are the best rational approximations

Let p_n/q_n be the n–th convergent of the continued fraction expansion of an irrational number x.

Theorem. Let a/b be any rational number such that $1 \le b \le q_n$. Then :

$$|q_n x - p_n| \le |bx - a|$$

with equality if and only if $(a, b) = (p_n, q_n)$.

Corollary. For $1 \le b \le q_n$ we have

$$\left| x - \frac{p_n}{q_n} \right| \le \left| x - \frac{a}{b} \right|$$

with equality if and only if $(a, b) = (p_n, q_n)$.

Legendre Theorem

Adrien–Marie Legendre

(1752 – 1833)

If

$$\left| x - \frac{p}{q} \right| \le \frac{1}{2q^2},$$

then p/q is a convergent of x.

Lagrange Theorem

Lagrange

(1736 – 1813)

The continued fraction expansion of a real irrational number x *is ultimately periodic if and only if* x *is quadratic.*

Diophantus of Alexandria (250 ±50)

Rational approximation

The rational numbers are dense in the real numbers :
For any x in $\mathbf{R}$ and any $\epsilon > 0$, there exists $p/q \in \mathbf{Q}$ such that

$$\left| x - \frac{p}{q} \right| < \epsilon.$$

Numerical approximation : starting from the rational numbers, compute the maximal number of digits of x with the minimum number of operations (notion of complexity).

Rational approximation : given x and ϵ, find p/q with q minimal such that $|x - p/q| < \epsilon$.

Rational approximation

The rational numbers are dense in the real numbers :
For any x in $\mathbf{R}$ and any $\epsilon > 0$, there exists $p/q \in \mathbf{Q}$ such that

$$\left| x - \frac{p}{q} \right| < \epsilon.$$

Numerical approximation : starting from the rational numbers, compute the maximal number of digits of x with the minimum number of operations (notion of complexity).

Rational approximation : given x and ϵ, find p/q with q minimal such that $|x - p/q| < \epsilon$.

Rational approximation

The rational numbers are dense in the real numbers :
For any x in $\mathbf{R}$ and any $\epsilon > 0$, there exists $p/q \in \mathbf{Q}$ such that

$$\left| x - \frac{p}{q} \right| < \epsilon.$$

Numerical approximation : starting from the rational numbers, compute the maximal number of digits of x with the minimum number of operations (notion of complexity).

Rational approximation : given x and ϵ, find p/q with q minimal such that $|x - p/q| < \epsilon$.

Rational approximation to real numbers

Easy : for any $x \in \mathbf{R}$ and any $q \geq 1$, there exists $p \in \mathbf{Z}$ with $|qx - p| \leq 1/2$.

Solution : take for p the nearest integer to qx.

This inequality

$$\left| x - \frac{p}{q} \right| < \frac{1}{2q}$$

is best possible when qx is half an integer. We want to investigate stronger estimates : hence we need to exclude rational numbers.

Rational approximation to real numbers

Easy : for any $x \in \mathbf{R}$ and any $q \geq 1$, there exists $p \in \mathbf{Z}$ with $|qx - p| \leq 1/2$.
Solution : take for p the nearest integer to qx.

This inequality

$$\left| x - \frac{p}{q} \right| < \frac{1}{2q}$$

is best possible when qx is half an integer. We want to investigate stronger estimates : hence we need to exclude rational numbers.

Rational approximation to real numbers

Easy : for any $x \in \mathbf{R}$ and any $q \geq 1$, there exists $p \in \mathbf{Z}$ with $|qx - p| \leq 1/2$.
Solution : take for p the nearest integer to qx.

This inequality

$$\left| x - \frac{p}{q} \right| < \frac{1}{2q}$$

is best possible when qx is half an integer. We want to investigate stronger estimates : hence we need to exclude rational numbers.

Rational approximation to rational numbers

A rational number has an excellent rational approximation : itself !

But there is no other good approximation : if x is rational, there exists a constant $c = c(x) > 0$ such that, for any $p/q \in \mathbf{Q}$ with $p/q \neq x$,

$$\left| x - \frac{p}{q} \right| \geq \frac{c}{q}.$$

Proof : Write $x = a/b$ and set $c = 1/b$: since $aq - bp$ is a nonzero integer, it has absolute value at least 1, and

$$\left| x - \frac{p}{q} \right| = \frac{|aq - bp|}{bq} \geq \frac{1}{bq}$$

Rational approximation to rational numbers

A rational number has an excellent rational approximation : itself !
But there is no other good approximation : if x is rational, there exists a constant $c = c(x) > 0$ such that, for any $p/q \in \mathbf{Q}$ with $p/q \neq x$,

$$\left| x - \frac{p}{q} \right| \geq \frac{c}{q}.$$

Proof : Write $x = a/b$ and set $c = 1/b$: since $aq - bp$ is a nonzero integer, it has absolute value at least 1, and

$$\left| x - \frac{p}{q} \right| = \frac{|aq - bp|}{bq} \geq \frac{1}{bq}.$$

Rational approximation to rational numbers

A rational number has an excellent rational approximation : itself !
But there is no other good approximation : if x is rational, there exists a constant $c = c(x) > 0$ such that, for any $p/q \in \mathbf{Q}$ with $p/q \neq x$,

$$\left| x - \frac{p}{q} \right| \geq \frac{c}{q}.$$

Proof : Write $x = a/b$ and set $c = 1/b$: since $aq - bp$ is a nonzero integer, it has absolute value at least 1, and

$$\left| x - \frac{p}{q} \right| = \frac{|aq - bp|}{bq} \geq \frac{1}{bq}$$

Criterion for irrationality

Consequence. *Let* $\vartheta \in \mathbf{R}$. *Assume that for any* $\epsilon > 0$, *there exists* $p/q \in \mathbf{Q}$ *with*

$$0 < |q\vartheta - p| < \epsilon.$$

Then ϑ *is irrational.*

Rational approximation to irrational real numbers

Any irrational real number x has much better rational approximations than those of order $1/q$, namely there exist approximations of order $1/q^2$ (hence p will always be the nearest integer to qx).

For any $x \in \mathbf{R} \setminus \mathbf{Q}$, there exists infinitely many p/q with

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{q^2}.$$

Rational approximation to irrational real numbers

Any irrational real number x has much better rational approximations than those of order $1/q$, namely there exist approximations of order $1/q^2$ (hence p will always be the nearest integer to qx).

For any $x \in \mathbf{R} \setminus \mathbf{Q}$, there exists infinitely many p/q with

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{q^2}.$$