October 16, 2024

University of the Punjab, Lahore

Diophantine equations

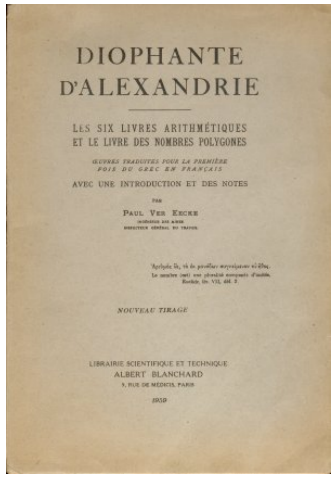
Michel Waldschmidt

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

Abstract

Given a polynomial in several variables with rational integer coefficients, we investigate the set of integer tuples where this polynomial vanishes. One of the best know examples is Fermat's equation $x^n + y^n = z^n$. Another family is given by the so–called Pell–Fermat equations $x^2 - dy^2 = \pm 1$ already considered by Brahmagupta (598 - 670) and Bhāskārāchārya (1114 - 1185). After a short historical survey on this subject starting with Hilbert's 10th Problem, we describe the state of the art concerning integer points on curves $f(x, y) = k$, including work of Thue, Siegel, Gel'fond, Baker, Schmidt.

Diophantus of Alexandria ($\sim 250 \pm 50$)



Diophantine quadruples : $(1, 3, 8, 120)$ $xy + 1$ is a square :
$4 = 2^2$, $9 = 3^2$, $121 = 11^2$, $25 = 5^2$, $361 = 19^2$, $961 = 31^2$.

G. H. Hardy and E. M. Wright, An introduction to the theory of numbers, Oxford University Press, Oxford, sixth ed., 2008.
Revised by D. R. Heath-Brown and J. H. Silverman.

https://mathshistory.st-andrews.ac.uk/Biographies/Diophantus/

Diophantus of Alexandria : example

Find an integer n such that $10n + 9$ and $5n + 4$ are squares :

$$x^2 = 10n + 9, \quad y^2 = 5n + 4$$

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

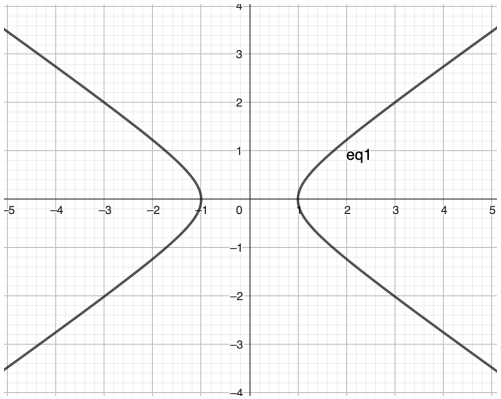
$n = 0$, $(x, y) = (3, 2)$, $x^2 = 9$, $y^2 = 4$.

$n = 28$, $(x, y) = (17, 12)$, $x^2 = 289$, $y^2 = 144$, $2y^2 = 288$.

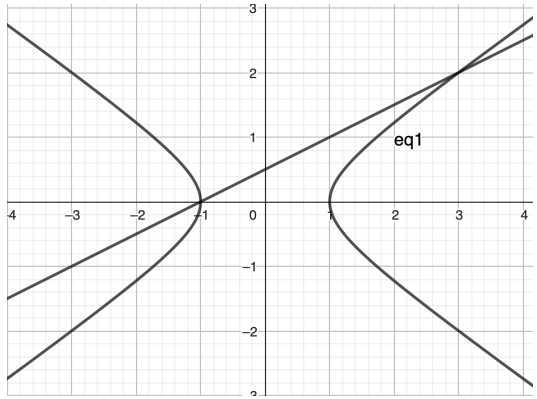
$n = 33\,292$, $(x, y) = (577, 408)$,
$x^2 = 332\,929$, $y^2 = 166\,464$, $2y^2 = 332\,928$.

Next ones : $n = 1\,130,976$, $n = 13\,051\,463\,040$.

Rational solutions to $x^2 - 2y^2 = 1$



$$y = t(x+1), t \in \mathbb{Q}$$



$$2t^2(x+1)^2 = x^2 - 1,$$
$$2t^2(x+1) = x - 1,$$

$$x = \frac{1+2t^2}{1-2t^2}, \quad y = \frac{2t}{1-2t^2}.$$

$$t = \frac{2}{3}, \quad 1-2t^2 = \frac{1}{9}, \quad 1+2t^2 = \frac{17}{9}, \quad (x,y) = (17,12).$$

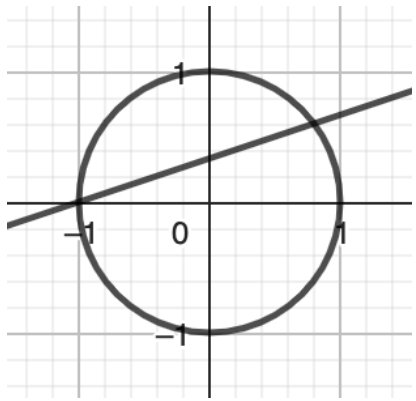
Pythagorean triples

Euclid

$\sim$325 BC – $\sim$ 265 BC

Parametrisation of the circle :
$x^2 + y^2 = 1$
rational points on the circle
$y = t(x + 1)$:

$$x = \frac{t^2 - 1}{t^2 + 1}, \quad y = \frac{2t}{t^2 + 1}.$$



Pythagoras equation $a^2 + b^2 = c^2$ (ref. : Hardy and Wright)
$m > n > 0$,

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2.$$

Integer solutions to $x^2 - 2y^2 = 1$

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

Pell–Fermat equation

$$(x, y) = (3, 2)$$

$$(3 + 2\sqrt{2})^2 = 17 + 12\sqrt{2}, \quad 17^2 - 2 \cdot 12^2 = 289 - 288 = 1.$$

$$(3+2\sqrt{2})^3 = 99+70\sqrt{2}, \quad 99^2 - 2 \cdot 70^2 = 9801 - 2 \cdot 4000 = 1.$$

$$(3+2\sqrt{2})^5 = 577+408\sqrt{2}, \quad 577^2 - 2 \cdot 408^2 = 232\,929 - 2 \cdot 166\,464 = 1.$$

An interesting street number

The puzzle itself was about a street in the town of Louvain in Belgium, where houses are numbered consecutively. One of the house numbers had the peculiar property that the total of the numbers lower than it was exactly equal to the total of the numbers above it. Furthermore, the mysterious house number was greater than 50 but less than 500.

Prasanta Chandra Mahalanobis

1893 – 1972

Srinivasa Ramanujan

1887 – 1920

http://mathshistory.st-andrews.ac.uk/Biographies/Mahalanobis.html

https://www.math.auckland.ac.nz/~butcher/miniature/miniature2.pdf

Street number : examples

Examples :

- House number 6 in a street with 8 houses :

$$1+2+3+4+5=15, \quad 7+8=15.$$

- House number 35 in a street with 49 houses. To compute

$$S := 1+2+3+\cdots+32+33+34$$

write

$$S = 34+33+32+\cdots+3+2+1$$

so that $2S = 34 \times 35$:

$$1+2+3+\cdots+34 = \frac{34\times 35}{2} = 595.$$

On the other side of the house,

$$36+37+\cdots+49 = \frac{49\times 50}{2} - \frac{35\times 36}{2} = 1225-630 = 595.$$

Other solutions to the puzzle

- House number 1 in a street with 1 house.
- House number 0 in a street with 0 house.

Ramanujan : *if no banana is distributed to no student, will each student get a banana ?*

The puzzle requests the house number between 50 and 500.

Street number

Let m be the house number and n the number of houses :

$$1 + 2 + 3 + \cdots + (m-1) = (m+1) + (m+2) + \cdots + n.$$

$$\frac{m(m-1)}{2} = \frac{n(n+1)}{2} - \frac{m(m+1)}{2}.$$

This is $2m^2 = n(n+1)$. Complete the square on the right :

$$8m^2 = (2n+1)^2 - 1.$$

Set $x = 2n+1$, $y = 2m$. Then

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

Infinitely many solutions to the puzzle

Ramanujan said he has infinitely many solutions (but a single one between 50 and 500).
Sequence of balancing numbers (number of the house)
https://oeis.org/A001109

$$0, 1, 6, 35, \mathbf{204}, 1189, 6930, 40391, 235416, 1372105, 7997214 \ldots$$

This is a linear recurrence sequence $u_{n+1} = 6u_n - u_{n-1}$ with the initial conditions $u_0 = 0$, $u_1 = 1$.

The number of houses is https://oeis.org/A001108

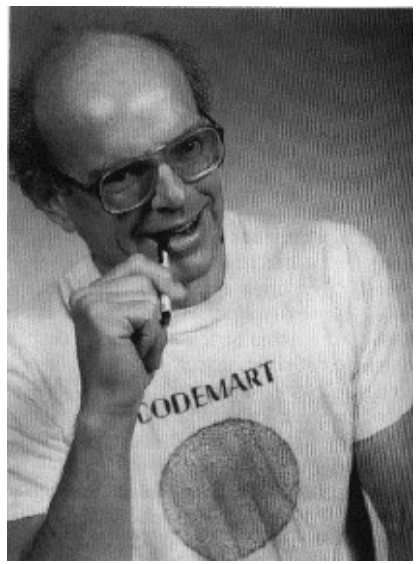
$$0, 1, 8, 49, \mathbf{288}, 1681, 9800, 57121, 332928, 1940449, \ldots$$

OEIS

The OEIS Foundation is supported by donations from users of the OEIS and by a grant from the Simons Foundation.

0 1 3 6 2 7 13 20 12 23 10 22 11 21 THE ON-LINE ENCYCLOPEDIA OF INTEGER SEQUENCES ®

founded in 1964 by N. J. A. Sloane



Neil J. A. Sloane's encyclopaedia

http://oeis.org/A001597 http://oeis.org/A001333

Brahmagupta (598 – 670)

Brāhmasphuṭasiddhānta : Solve in integers the equation

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

The smallest solution is

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

Composition method : *samasa* – Brahmagupta identity

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

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

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

Bhāskara II or Bhāskārāchārya (1114 - 1185)

Līlāvatī Ujjain (India)

Bijaganita, (1150)

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

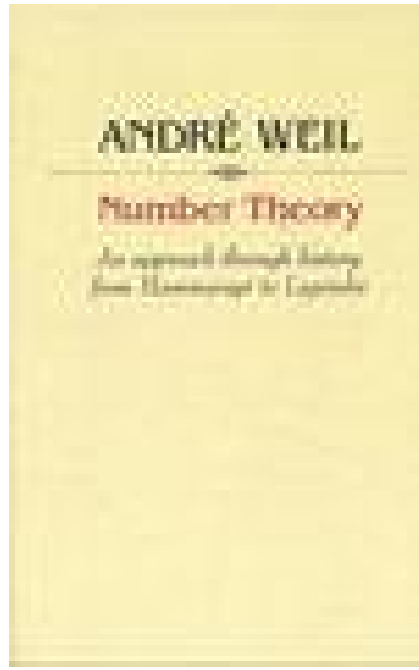
$$x = 1\,766\,319\,049, \qquad y = 226\,153\,980.$$

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

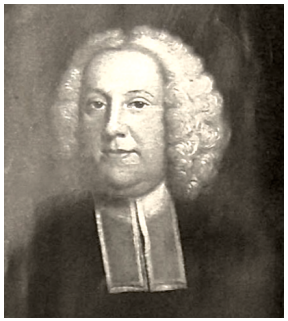
http://www-history.mcs.st-andrews.ac.uk/HistTopics/Pell.html

Reference to Indian mathematics

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



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



John Pell

1610 – 1685

It is often said that Euler mistakenly attributed Brouncker's work on this equation to Pell. However the equation appears in a book by Rahn which was certainly written with Pell's help : some say entirely written by Pell. Perhaps Euler knew what he was doing in naming the equation.

Johann Rahn (1622 - 1676) was a Swiss mathematician who was the first to use the symbol $\div$ for division.

https://mathshistory.st-andrews.ac.uk/Biographies/Pell/
https://fr.wikipedia.org/wiki/John_Pell

On the equation $x^2 - dy^2 = \pm 1$: history

Lord William Brouncker
1620–1684

Pierre de Fermat
1601–1665

Correspondence from Pierre de Fermat to Brouncker.

1657 : letter of Fermat to Frenicle de Bessy (1604–1674).

https://mathshistory.st-andrews.ac.uk/Biographies/

History (continued)

Leonard Euler

1707–1783

Joseph–Louis Lagrange

1736–1813

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

The complete theory of the equation $x^2 - dy^2 = \pm 1$ was worked out by Lagrange.

https://mathshistory.st-andrews.ac.uk/Biographies/

Solution of the equation $x^2 - dy^2 = \pm 1$

Let d be a positive integer, not a square. Then the equation $x^2 - dy^2 = \pm 1$ has infinitely many non negative solutions in integers (x, y).

There is a smallest positive *fundamental solution* (x_1, y_1) such that all non negative solutions are obtained by writing

$$x_\nu + y_\nu \sqrt{d} = (x_1 + y_1 \sqrt{d})^\nu$$

with $\nu \geqslant 0$.

The trivial solution $(x, y) = (1, 0)$ is obtained with $\nu = 0$.

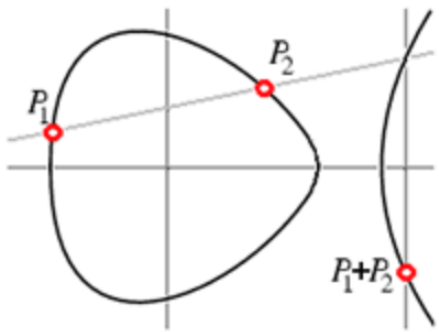
The set of solutions (x, y) in $\mathbb{Z} \times \mathbb{Z}$ is given by

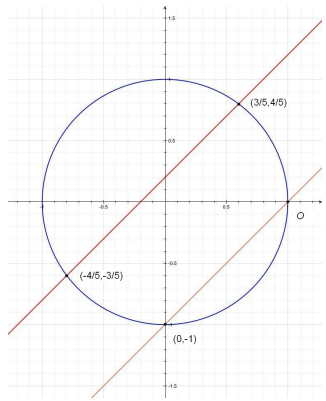
$$x_\nu + y_\nu \sqrt{d} = \pm (x_1 + y_1 \sqrt{d})^\nu$$

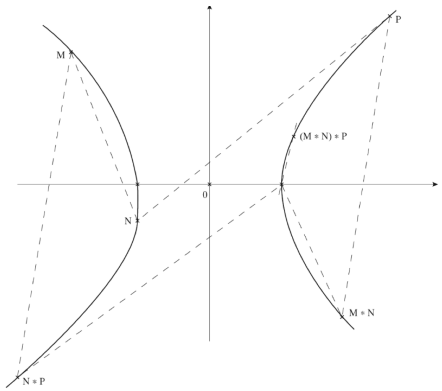
with $\nu \in \mathbb{Z}$. They form a group $\simeq \{\pm 1\} \times \mathbb{Z}$.

Group law on a conic

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







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

Mahalanobis puzzle $x^2 - 2y^2 = 1$, $x = 2n+1$, $y = 2m$

Fundamental solution : $(x_1, y_1) = (3, 2)$.
Other solutions (x_ν, y_ν) with

$$x_\nu + y_\nu\sqrt{2} = (3 + 2\sqrt{2})^\nu.$$

- $\nu = 0$, trivial solution : $x = 1$, $y = 0$, $m = n = 0$.
- $\nu = 1$, $x_1 = 3$, $y_1 = 2$, $m = n = 1$.
- $\nu = 2$, $x_2 = 17$, $y_2 = 12$, $n = 8$, $m = 6$,

$$x_2 + y_2\sqrt{2} = (3 + 2\sqrt{2})^2 = 17 + 12\sqrt{2}.$$

- $\nu = 3$, $x_3 = 99$, $y_3 = 70$, $n = 49$, $m = 35$,

$$x_3 + y_3\sqrt{2} = (3 + 2\sqrt{2})^3 = 99 + 70\sqrt{2}.$$

Diophantus problem

Find an integer n such that $10n + 9$ and $5n + 4$ are squares :

$$x^2 = 10n + 9, \quad y^2 = 5n + 4$$

$$x^2 - 2y^2 = 1 \qquad \texttt{http://oeis.org/A001333}$$

$$1,\ 3,\ 17,\ 99,\ 577,\ 3\,363,\ 19\,601,\ 114\,243,\ 665\,857,\ 3\,880\,899,\ \ldots$$

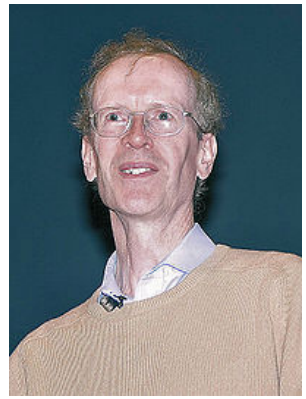
$$x = 3, \quad 17, \quad 577, \quad 3\,363, \quad 114\,243, \ldots$$

$$n = \frac{x^2 - 9}{10} = 0, \quad 28, \quad 33\,292, \quad 1\,130,976, \quad 1\,305\,146\,304 \ldots$$

Pierre de Fermat

Pierre de Fermat

1601–1665



Andrew Wiles

Proof of Fermat's last Theorem by Andrew Wiles (1993) : for $n \geqslant 3$, there is no positive integer solution (a, b, c) to

$$a^n + b^n = c^n.$$

Ramanujan – Nagell Equation

Srinivasa Ramanujan

1887 – 1920

Trygve Nagell

1895 – 1988

Ramanujan – Nagell Equation

$$x^2 + 7 = 2^n$$

$$\begin{aligned}
1^2 + 7 &= 2^3 &&= 8 \\
3^2 + 7 &= 2^4 &&= 16 \\
5^2 + 7 &= 2^5 &&= 32 \\
11^2 + 7 &= 2^7 &&= 128 \\
181^2 + 7 &= 2^{15} &&= 32\,768
\end{aligned}$$

$x^2 + D = 2^n$

Nagell (1948) : for $D = 7$, no further solution

Apéry (1960) : for $D > 0$, $D \neq 7$, the equation $x^2 + D = 2^n$ has at most 2 solutions.

Roger Apéry

1916 – 1994

Examples with 2 solutions :

$$D = 23 : \qquad 3^2 + 23 = 32, \quad 45^2 + 23 = 2^{11} = 2\,048$$

$$D = 2^{\ell+1} - 1,\ \ell \geqslant 3 : \qquad (2^\ell - 1)^2 + 2^{\ell+1} - 1 = 2^{2\ell}$$

$x^2 + D = 2^n$

Beukers (1980) : at most one solution otherwise.

Frits Beukers

Mike Bennett

M. Bennett (1995) : considers the case $D < 0$.

Diophantine equations : early historical survey

Pierre Fermat (1601 ? – 1665)

Leonhard Euler (1707 – 1783)

Joseph Louis Lagrange (1736 – 1813)

XIXth Century : Adolf Hurwitz, Henri Poincaré





Hilbert's 8th Problem

David Hilbert
1862 – 1943

Second International Congress of Mathematicians in Paris. August 8, 1900

Twin primes,

Goldbach's Conjecture,

Riemann Hypothesis

http://www.maa.org/sites/default/files/pdf/upload$_-$library/22/Ford/Thiele1-24.pdf

Hilbert's tenth problem

D. Hilbert (1900) — *Problem :* to give an algorithm in order to decide whether a diophantine equation has an integer solution or not.

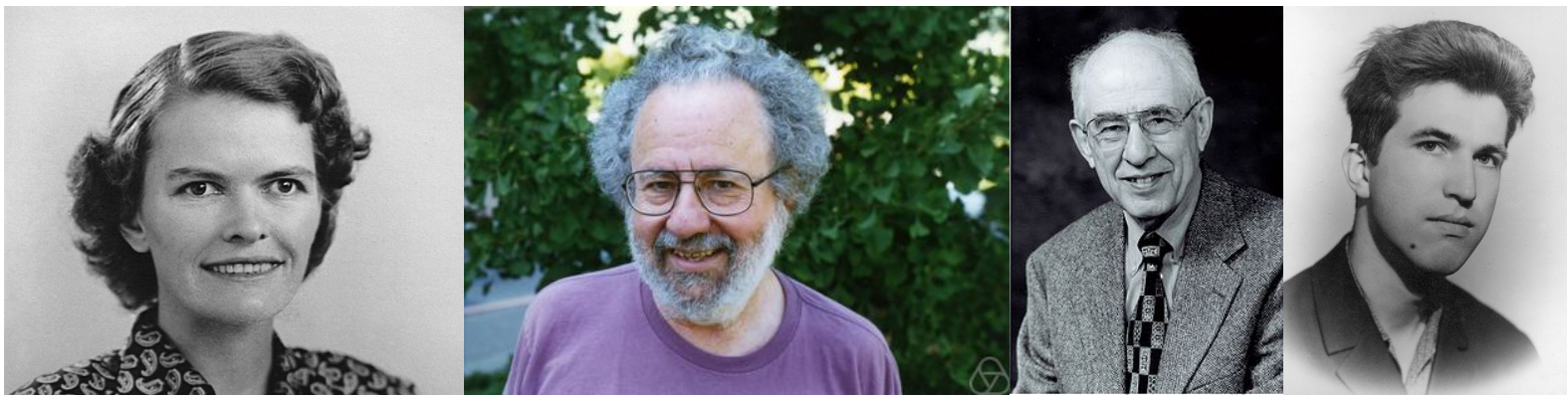
If we do not succeed in solving a mathematical problem, the reason frequently consists in our failure to recognize the more general standpoint from which the problem before us appears only as a single link in a chain of related problems. After finding this standpoint, not only is this problem frequently more accessible to our investigation, but at the same time we come into possession of a method which is applicable also to related problems.

Negative solution to Hilbert's 10th problem

Julia Robinson (1952)

Julia Robinson, Martin Davis, Hilary Putnam (1961)

Yuri Matijasevic (1970)



Remark : the analog for *rational points* of Hilbert's 10th problem is not yet solved :
Does there exist an algorithm in order to decide whether a Diophantine equation has a rational solution or not ?

Diophantine equations : historical survey

Thue (1908) : there are only finitely many integer solutions of

$$F(x, y) = m,$$

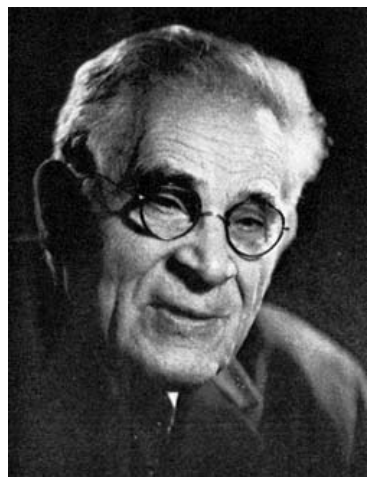
when F is homogeneous irreducible form over $\mathbb{Q}$ of degree $\geqslant 3$.

Mordell's Conjecture (1922) : rational points on algebraic curves

Siegel's Theorem (1929) : integral points on algebraic curves

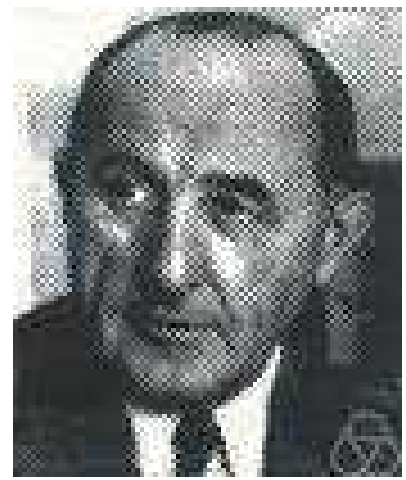
Axel Thue

1863 - 1922



Louis Mordell

1888 – 1972

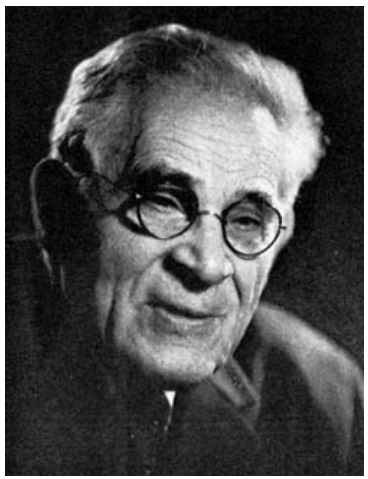


Carl Ludwig Siegel

1896 - 1981

Mordell's Conjecture, Faltings's Theorem

Mordell's Conjecture : 1922. Faltings's Theorem (1983). The set of rational points on a number field of a curve of genus $\geqslant 2$ is finite.



Louis Mordell

1888 – 1972

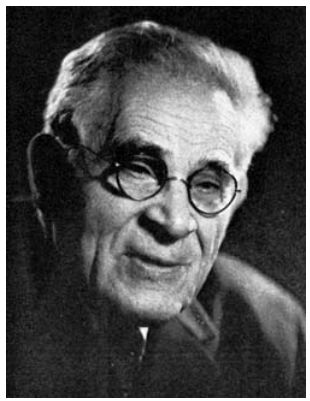
Gerd Faltings

The group of rational points on an elliptic curve

Conjecture (Henri Poincaré, 1901) : finitely many points are sufficient to deduce all rational points by the chord and tangent method.

Henri Poincaré

1854 – 1912



Louis Mordell

1888 – 1972

Theorem (Mordell, 1922). *If E is an elliptic curve over $\mathbb{Q}$, then the abelian group $E(\mathbb{Q})$ is finitely generated : there exists a nonnegative integer r (the* Mordell-Weil rank *of the curve over $\mathbb{Q}$) such that*

$$E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$$

Mordell–Weil Theorem

André Weil (1928) : generalization to number fields and abelian varieties :

If A is an Abelian variety over a number field K, then the abelian group $A(K)$ is finitely generated :

$$A(K) = A(K)_{\text{tors}} \times \mathbb{Z}^r$$

with $r \geqslant 0$ while $A(K)_{\text{tors}}$ is a finite group.

Jacques Hadamard

1865 - 1963

André Weil

1906 – 1998

Weil's thesis : 1928. Hadamard's comment.

Reference : Antoine Chambert-Loir. *La conjecture de Mordell : origines, approches, généralisations.* Séminaire Betty B., Septembre 2021 5e année, 2021–2022

Axel Thue

Axel Thue
1863 - 1922

Thue (1908) : there are only finitely many integer solutions of

$$F(x, y) = m,$$

when F is homogeneous irreducible form over $\mathbb{Q}$ of degree $\geqslant 3$.

Liouville's inequality (1844)

Liouville's inequality . *Let* α *be an algebraic number of degree* $d \geqslant 2$. *There exists* $c(\alpha) > 0$ *such that, for any* $p/q \in \mathbb{Q}$ *with* $q > 0$,

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^d}.$$

Joseph Liouville
1809–1882

Liouville's estimate for $\sqrt[3]{2}$:

For any $p/q \in \mathbb{Q}$,

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{1}{6q^3}.$$

Proof.
Since $\sqrt[3]{2}$ is irrational, for p and q rational integers with $q > 0$, we have $p^3 - 2q^3 \neq 0$, hence

$$|p^3 - 2q^3| \geqslant 1.$$

Write

$$p^3 - 2q^3 = (p - \sqrt[3]{2}q)(p^2 + \sqrt[3]{2}pq + \sqrt[3]{4}q^2).$$

If $p \leqslant (3/2)q$, then

$$p^2 + \sqrt[3]{2}pq + \sqrt[3]{4}q^2 < 6q^2.$$

Hence

$$1 \leqslant 6q^2|p - \sqrt[3]{2}q|.$$

Liouville's estimate for $\sqrt[3]{2}$:

For any $p/q \in \mathbb{Q}$,

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{1}{6q^3}.$$

Proof.
We completed the proof in the case $p \leqslant (3/2)q$.
If $p > (3/2)q$, then

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{3}{2} - \sqrt[3]{2} > \frac{1}{6}.$$

Improving Liouville's inequality

If we can improve the lower bound

$$|p^3 - 2q^3| \geqslant 1,$$

then we can improve Liouville's estimate

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{1}{6q^3}.$$

What turns out to be much more interesting is the converse :
If we can improve Liouville's estimate

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{1}{6q^3},$$

then we can improve the lower bound

$$|p^3 - 2q^3| \geqslant 1.$$

Improvements of Liouville's inequality

In the lower bound

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^d}$$

for α real algebraic number of degree $d \geqslant 3$, the exponent d of q in the denominator of the right hand side was replaced by κ with

- any $\kappa > (d/2) + 1$ by A. Thue (1909),
- $2\sqrt{d}$ by C.L. Siegel in 1921,
- $\sqrt{2d}$ by F.J. Dyson and A.O. Gel'fond in 1947,
- any $\kappa > 2$ by K.F. Roth in 1955.

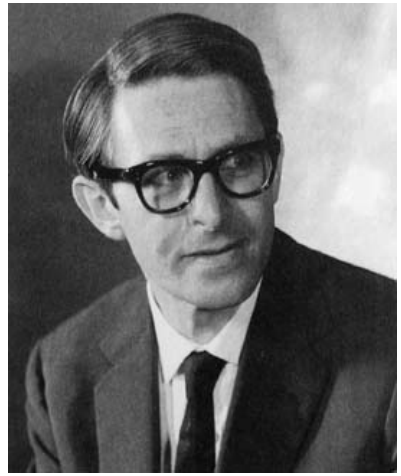
Thue– Siegel– Roth Theorem

Axel Thue

1863 - 1922

Carl Ludwig Siegel

1896 - 1981



Klaus Friedrich Roth

1925 – 2015

For any real algebraic number α*, for any* $\epsilon > 0$*, the set of* $p/q \in \mathbb{Q}$ *with* $|\alpha - p/q| < q^{-2-\epsilon}$ *is finite.*

Thue– Siegel– Roth Theorem

An equivalent statement is that, for any real algebraic irrational number α and for any $\epsilon > 0$, there exists $q_0 > 0$ such that, for $p/q \in \mathbb{Q}$ with $q \geqslant q_0$, we have

$$|\alpha - p/q| > q^{-2-\epsilon}.$$

Thue equation and Diophantine approximation

Liouville's estimate for the rational Diophantine approximation of $\sqrt[3]{2}$:

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{1}{9q^3}$$

for sufficiently large q.

Mike Bennett (1997) : *for any* $p/q \in \mathbb{Q}$,

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| \geqslant \frac{1}{4\ q^{2.5}}.$$

Mike Bennett

http://www.math.ubc.ca/~bennett/

For any $p/q \in \mathbb{Q}$,

$$\left| \sqrt[3]{2} - \frac{p}{q} \right| \geqslant \frac{1}{4\ q^{2.5}}.$$

For any $(x, y) \in \mathbb{Z}^2$ *with* $x > 0$,

$$|x^3 - 2y^3| \geqslant \sqrt{x}.$$

Connection between Diophantine approximation and Diophantine equations

Let κ satisfy $0 < \kappa \leqslant 3$.
The following conditions are equivalent :
(i) There exists $c_1 > 0$ *such that*

$$\left| \sqrt[3]{2} - \frac{p}{q} \right| \geqslant \frac{c_1}{q^\kappa}$$

for any $p/q \in \mathbb{Q}$.
(ii) There exists $c_2 > 0$ *such that*

$$|x^3 - 2y^3| \geqslant c_2 \, x^{3-\kappa}$$

for any $(x, y) \in \mathbb{Z}^2$ *having* $x > 0$.

Thue's equation and approximation

Let $f \in \mathbb{Z}[X]$ be an irreducible polynomial of degree d and let $F(X,Y) = Y^d f(X/Y)$ be the associated homogeneous binary form of degree d. Then the following two assertions are equivalent :

(i) For any integer $k \neq 0$, the set of $(x,y) \in \mathbb{Z}^2$ verifying

$$F(x,y) = k$$

is finite.

(ii) For any real number $\kappa > 0$ and for any root $\alpha \in \mathbb{C}$ of f, the set of rational numbers p/q verifying

$$\left|\alpha - \frac{p}{q}\right| \leqslant \frac{\kappa}{q^d}$$

is finite.

Thue equation

Condition (i) above :

For any integer $k \neq 0$, the set of $(x, y) \in \mathbb{Z}^2$ verifying

$$F(x, y) = k$$

is finite.

can also be phrased by stating that for any positive integer k, the set of $(x, y) \in \mathbb{Z}^2$ verifying

$$0 < |F(x, y)| \leqslant k$$

is finite.

Schmidt's Subspace Theorem (1970)

For $m \geqslant 2$ let $L_0, \ldots, L_{m-1}$ be m independent linear forms in m variables with algebraic coefficients. Let $\epsilon > 0$. Then the set

$$\{\mathbf{x} = (x_0, \ldots, x_{m-1}) \in \mathbb{Z}^m \; ;$$

$$|L_0(\mathbf{x}) \cdots L_{m-1}(\mathbf{x})| \leqslant |\mathbf{x}|^{-\epsilon}\}$$

is contained in the union of finitely many proper subspaces of $\mathbb{Q}^m$.

Wolfgang M. Schmidt

Effectivity

The Theorem of Thue–Siegel–Roth–Schmidt is not effective : upper bounds for the number of solutions can be derived, but no upper bound for the solutions themselves.

Faltings's Theorem is not effective : so far, there is no known effective bound for the solutions $(x, y) \in \mathbb{Q}^2$ of a Diophantine equation $f(x, y) = 0$, where $f \in \mathbb{Z}[X, Y]$ is a polynomial such that the curve $f(x, y) = 0$ has genus $\geqslant 2$.

Even for integral points, there is no effective version of Siegel's Theorem on integral points on a curve of genus $\geqslant 2$.

Number of solutions

G. Rémond (2000) : explicit upper bound for the number of solutions in Faltings's Theorem.

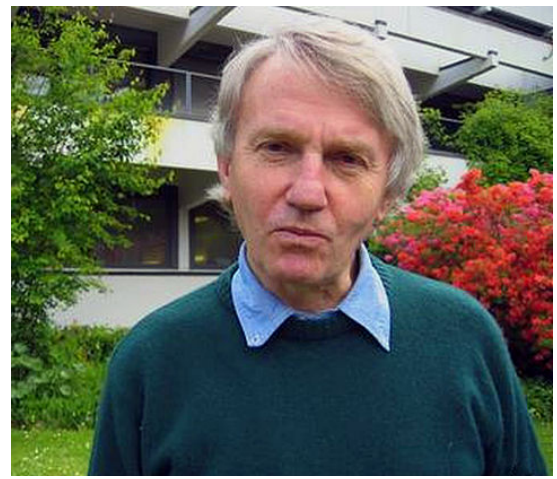
Gaël Rémond

Effective version of Siegel's Theorem (genus 1)

A. Baker and J. Coates. Integer points on curves of genus 1. Proc. Camb. Philos. Soc. 67, 595–602 (1970).

Alan Baker

1939 – 2018



John Coates

(1945 – 2022)

Gel'fond–Baker method

While Thue's method was based on the non effective Thue–Siegel–Roth Theorem, Baker and Fel'dman followed an effective method introduced by A.O. Gel'fond, involving *lower bounds for linear combinations of logarithms of algebraic numbers with algebraic coefficients.*

Alexandre Ossipovitch Gel'fond

1906–1968

Alan Baker

1939 – 2018

Lower bound for linear combinations of logarithms

A lower bound for a nonvanishing difference

$$\alpha_1{}^{b_1} \cdots \alpha_n{}^{b_n} - 1$$

is essentially the same as a lower bound for a nonvanishing number of the form

$$b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n,$$

since $e^z - 1 \sim z$ for $z \to 0$.
The first nontrivial lower bounds were obtained by A.O. Gel'fond. His estimates were effective only for $n = 2$: for $n \geqslant 3$, he needed to use estimates related to the Thue–Siegel–Roth Theorem.

Explicit version of Gel'fond's estimates

A. Schinzel (1968) computed explicitly the constants introduced by A.O. Gel'fond. in his lower bound for

$$\left|{\alpha_1}^{b_1}{\alpha_2}^{b_2} - 1\right|.$$

Andrzej Schinzel

1937–1921

He deduced explicit Diophantine results using the approach introduced by A.O. Gel'fond.

Alan Baker (1939 – 2018)

Alan Baker
1939 – 2018

In 1968, A. Baker succeeded to extend to any $n \geqslant 2$ the transcendence method used by A.O. Gel'fond for $n = 2$. As a consequence, effective upper bounds for the solutions of Thue's equations have been derived.

October 16, 2024

University of the Punjab, Lahore

Diophantine equations

Michel Waldschmidt

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