

 BUSHRA MATEEN BUILDING

calling for
APPLICATIONS
CIMPA School 2027

**SYMBOLIC DYNAMICS IN
CONNECTION WITH
COMBINATORICS ON WORDS,
NUMBER THEORY AND GEOMETRY**

 Lahore, Pakistan

 March 15th -
March 26th, 2027

Application Deadline:
November 15th, 2026 

For more information:
www.cimpa.info/en/node/63

 www.cimpa.info  CIMPA Math  [cima.math](https://www.instagram.com/cimpa.math)
CIMPA - Centre International de Mathématiques Pures et Appliquées

October 28th - November 1st, 2026

October 30, 2026

Souphanouvong University, Luang Prabang, Lao PDR.

**13th International Conference on Mathematics
and Mathematics Education in Developing Countries
(ICMMEDC2026)**

A brief history of Diophantine equations

Michel Waldschmidt

Professeur Émérite, Sorbonne Université,
Institut de Mathématiques de Jussieu, Paris

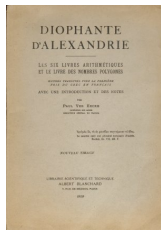
<http://www.imj-prg.fr/~michel.waldschmidt/>

Abstract

A *Diophantine equation* is an equation where the unknowns are rational integers or rational numbers. Most often it is an equation $F(x_1, \dots, x_n) = 0$ where F is a polynomial. Such equations were studied as early as around the third century by the Greek mathematician [Diophantus of Alexandria](#) whose name was given to them. Among the oldest examples of such equations are those which were studied by Indian astronomers like [Brahmagupta](#) (598 – 670) and [Bhaskara II](#) (1114 - 1185). The most famous Diophantine equation is $x^n + y^n = z^n$ considered by [Pierre de Fermat](#) (1601–1665) and solved by [Andrew Wiles](#) (1993).

According to the negative solution by [Yuri Matijasevic](#) (1970) of [Hilbert's](#) tenth problem, there is no general algorithm to decide whether a Diophantine equation has a solution in $\mathbb{Z}$. Nevertheless, there are many results on this question, including recent ones.

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



Diophantine equations
Diophantine approximation
Diophantine problems
Diophantine tuples

Main Theorem of Diophantine approximation : if a is a nonzero integer, then $|a| \geq 1$.

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

Rational Diophantine tuples

If x and y are two distinct elements among

$$\frac{1}{16}, \quad \frac{33}{16}, \quad \frac{17}{4}, \quad \frac{105}{16},$$

then $xy + 1$ is a square.

$$\begin{aligned} \frac{1}{16} \cdot \frac{33}{16} + 1 &= \left(\frac{17}{16}\right)^2, & \frac{1}{16} \cdot \frac{17}{4} + 1 &= \left(\frac{9}{8}\right)^2, \\ \frac{1}{16} \cdot \frac{105}{16} + 1 &= \left(\frac{19}{16}\right)^2, & \frac{33}{16} \cdot \frac{17}{4} + 1 &= \left(\frac{25}{8}\right)^2, \\ \frac{33}{16} \cdot \frac{105}{16} + 1 &= \left(\frac{61}{16}\right)^2, & \frac{17}{4} \cdot \frac{105}{16} + 1 &= \left(\frac{43}{8}\right)^2. \end{aligned}$$

Method of Diophantus of Alexandria

Four unknowns, six equations. The equation

$$y^2 = 9x^2 + 24x + 13$$

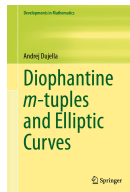
has the solution

$$x = \frac{1}{16}, \quad y = \frac{61}{16}.$$

$$61^2 = 3\,721 = 9 + 24 \cdot 16 + 13 \cdot 16^2.$$



Andrej Dujella



A Diophantine quadruple



Pierre de Fermat

1601–1665

Diophantine quadruple :

$(1, 3, 8, 120)$

$xy + 1$ is a square

$$\begin{aligned}1 \cdot 3 + 1 &= 4 = 2^2, & 1 \cdot 8 + 1 &= 9 = 3^2, & 1 \cdot 120 + 1 &= 121 = 11^2, \\3 \cdot 8 + 1 &= 25 = 5^2, & 3 \cdot 120 + 1 &= 361 = 19^2, \\8 \cdot 120 + 1 &= 961 = 31^2.\end{aligned}$$

Rational Diophantine quintuple



Leonard Euler
1707–1783

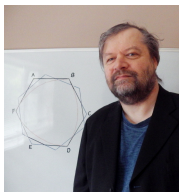
$$\left(1, 3, 8, 120, \frac{777480}{8288641}\right)$$

$$\frac{777480}{8288641} + 1 = \left(\frac{3011}{2879}\right)^2, \quad 3 \cdot \frac{777480}{8288641} + 1 = \left(\frac{3259}{2879}\right)^2,$$

$$8 \cdot \frac{777480}{8288641} + 1 = \left(\frac{3809}{2879}\right)^2,$$

$$120 \cdot \frac{777480}{8288641} + 1 = \left(\frac{10\,079}{2879}\right)^2.$$

Rational Diophantine sextuples



Philip Gibbs

Seven examples in

P.E. Gibbs,

Some Rational Diophantine Sextuples, (1999).

arxiv: math.NT/9902081

including

$$\frac{11}{192}, \quad \frac{35}{192}, \quad \frac{155}{27}, \quad \frac{512}{27}, \quad \frac{1235}{48}, \quad \frac{180\,873}{16}.$$

Five more examples in

P.E. Gibbs,

A generalised Stern-Brocot tree from regular Diophantine quadruples, (1999). arXiv: math.NT/9903035.

Diophantine quintuples in integers



Bo He



Alain Togbé



Volker Ziegler

Bo He, Alain Togbé and Volker Ziegler. *There is no Diophantine quintuple*. Trans. Amer. Math. Soc. **371**, 6665–6709 (2019).

Diophantus of Alexandria : another problem

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

Solutions

$$n = 0, 10n + 9 = 9 = 3^2, 5n + 4 = 4 = 2^2.$$

$$n = 28, 10n + 9 = 289 = 17^2, 5n + 4 = 144 = 12^2.$$

$$n = 33\,292, \\ 10n + 9 = 332\,929 = 577^2, \quad 5n + 4 = 166\,464 = 408^2.$$

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

Problem by Diophantus of Alexandria

$10n + 9$ and $5n + 4$ are squares :

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

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

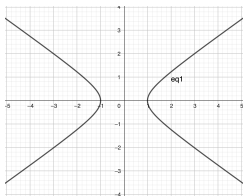
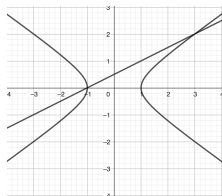
$$n = 0, (x, y) = (3, 2), x^2 = 9, y^2 = 4.$$

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

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

For $x = 99$, $y = 70$ we have $x^2 - 2y^2 = 9801 - 9800 = 1$ but this is not a solution to Diophantus problem : $x^2 = 980 \cdot 10 + 1$, $y^2 = 980 \cdot 5$.

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



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

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

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

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

$$t = \frac{1}{2}, \quad (x, y) = (3, 2).$$

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

Pythagorean triples



Euclid

~325 BC – ~265 BC

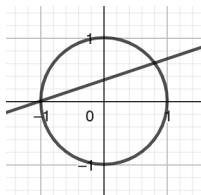
$$x = \frac{t^2 - 1}{t^2 + 1}, \quad y = \frac{2t}{t^2 + 1}.$$

Parametrisation of the circle :

$$x^2 + y^2 = 1$$

rational points on the circle

$$y = t(x + 1) :$$



Pythagoras equation $a^2 + b^2 = c^2$ (ref. : Hardy and Wright)

$m > n > 0$,

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

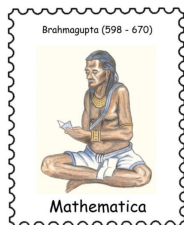
Brahmagupta (598 – 670)

Brāhmasphuṭasiddhānta
(628) :

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

The smallest solution is

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



Brahmagupta
598 – 670

Composition method : *samasa* – Brahmagupta identity

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

Bhāskara II or Bhāskarāchārya (1114 – 1185)

Lilavati Ujjain (India)

(*Bijagaṇita*, 1150)

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

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



Bhāskara II
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://www-history.mcs.st-andrews.ac.uk/HistTopics/Pell.html>
https://mathshistory.st-andrews.ac.uk/Biographies/Bhaskara_II/

Narayaṇa Paṇḍit $\sim$ 1340 – $\sim$ 1400

Author of *Gaṇita Kaumudī* on arithmetic in 1356.

Narayaṇa cows (*Tom Johnson*)

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

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

Reference to Indian mathematics

André Weil

Number theory :

An approach through history.

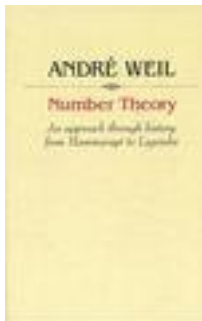
*From **Hammurapi** to*

***Legendre**.*

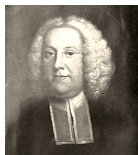
Birkhäuser Boston, Inc.,

Boston, Mass., (1984) 375 pp.

MR 85c:01004



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



John Pell
1610 – 1685



Johann Heinrich Rahn
1622 – 1676

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 Heinrich Rahn 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 $x^2 - dy^2 = \pm 1$: in Europ



Lord William Brouncker
1620–1684



Pierre de Fermat
1601–1665

Correspondence from Pierre de Fermat to Lord Brouncker.
1657 : letter of Fermat to Frenicle de Bessy (1604–1674).

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

Correspondence from Fermat to Lord Brouncker

“pour ne vous donner pas trop de peine” (Fermat)

“to make it not too difficult”

$$x^2 - dy^2 = 1, \text{ with } d = 61 \text{ and } d = 109.$$

Solutions respectively :

$$\begin{aligned} & (1\,766\,319\,049, 226\,153\,980) \\ & (158\,070\,671\,986\,249, 15\,140\,424\,455\,100) \end{aligned}$$

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

XVIII th Century



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/>

Diophantus problem

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

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

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

<http://oeis.org/A001333>

1, 3, 17, 99, 577, 3 363, 19 601, 114 243, 665 857, 3 880 899, ...

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

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

Pierre de Fermat



Pierre de Fermat

1601–1665



Andrew Wiles

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

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

Claude-Gaspard Bachet dit de Méziriac



Bachet de Méziriac

1581 – 1638

Latin translation of
Diophantus's Greek text
Arithmetica (1621)

Based on **Bombelli**'s Algebra and on a complete Latin translation by **Wilhelm Holzmann** (also known as **Xylander**) in 1575.

<https://mathshistory.st-andrews.ac.uk/Biographies/Bachet/>

Diophantine equations in Europe

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](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 was not solved before AI :

*Does there exist an algorithm in order to decide whether a Diophantine equation has a **rational** solution or not ?*

Rational and integer points on curves

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

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

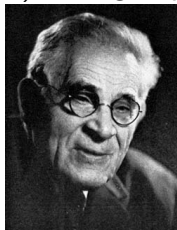
when F is homogeneous irreducible form over $\mathbb{Q}$ of degree ≥ 3 .

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



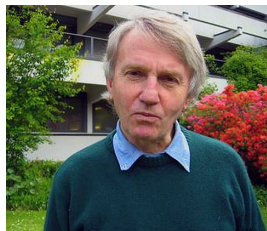
Carl Ludwig Siegel
1896 - 1981

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)

No algorithm is known so far for integer points on a curve of genus 2.

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*.



A.O. Gel'fond
1906–1968



A. Baker
1939 – 2018



N.I. Fel'dman
1918 – 1994

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 $z \rightarrow 0$.

The first nontrivial lower bounds were obtained by

A.O. Gel'fond. His estimates were effective only for $n = 2$: for $n \geq 3$, 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

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



Andrzej Schinzel

1937–1921

He deduced explicit Diophantine results using Gel'fond's approach.

Alan Baker (1939 – 2018)



Alan Baker
1939 – 2018

In 1968, A. Baker succeeded to extend to any $n \geq 2$ 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.

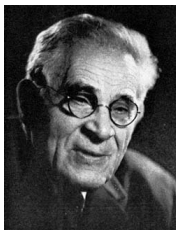
Diophantine equations

A.O. Gel'fond, A. Baker, V. Sprindžuk, K. Győry, M. Mignotte, R. Tijdeman, M. Bennett, P. Voutier, Y. Bugeaud, T.N. Shorey, S. Laishram...



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 ≥ 2 is finite.



Louis Mordell
1888 – 1972



Gerd Faltings

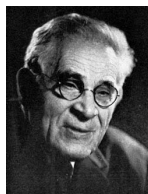
The group of rational points on an elliptic curve

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 :

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

with $r \geq 0$ 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

A one million US\$ open problem

Conjecture of Birch and Swinnerton-Dyer



Henry Peter Francis Swinnerton-Dyer (1927-2018)
and Bryan John Birch

B. Birch and H.P.F. Swinnerton-Dyer. *Notes on Elliptic Curves. II.*
J. reine angew. Math. **218**, 79–108 (1965).

Clay Mathematics Institute. *The Birch and Swinnerton-Dyer Conjecture.*
http://www.claymath.org/millennium/Birch_and_Swinnerton-Dyer_Conjecture/

October 28th - November 1st, 2026

October 30, 2026

Souphanouvong University, Luang Prabang, Lao PDR.

**13th International Conference on Mathematics
and Mathematics Education in Developing Countries
(ICMMEDC2026)**

A brief history of Diophantine equations

Michel Waldschmidt

Professeur Émérite, Sorbonne Université,
Institut de Mathématiques de Jussieu, Paris

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