THE ABEL PRIZE

Gerd Faltings
Abel Prize Laureate 2026

Rational solutions to Diophantine equations


Diophantus of Alexandria
(Photo: famousmathmaticians.net)

The expression Diophantine equation refers to Diophantus of Alexandria, a Hellenistic mathematician of the 3rd century. Diophantus was a pioneer in finding integer solutions to polynomial equations with integer coefficients, and his name has ever since been connected to finding integer and rational solutions to such equations.

The problem of finding rational solutions of polynomial equations dates several hundreds of years back in time. Already in ancient time, it was known that the Pythagorean equation $x^2 + y^2 = z^2$ has infinitely many integer solutions. The solutions are completely described by the formula

$$x = p^2 - q^2 \quad y = 2pq \quad z = p^2 + q^2$$

for two arbitrary positive integers p and q.

The Pythagorean equation is a quadratic equation, and the fact that there are infinitely many integer solutions can be viewed as a sign of the relatively frequent occurrence of squares among the integers. Increasing the degree of the equation will in general lead to a decreasing number of integer solutions. The number might drop from infinite to finite, and maybe also to zero, meaning that for a general equation with integer coefficients there are no integer solutions at all.


David Hilbert, 1862-1943
(Photo: Wikipedia)

At the International Congress of Mathematicians in Paris in 1900, the German mathematician David Hilbert put forth a list of 10 unsolved problems in mathematics. Later he published an extended list of 23 problems, all considered to be very influential for 20th-century mathematics. Some of the problems are still open, some has been solved. Hilbert introduces his 23 problems with the following words: ”Who of us would not be glad to lift the veil behind which the future lies hidden; to cast a glance at the next advances of our science and at the secrets of its development during future centuries? What particular goals will there be toward which the leading mathematical spirits of coming generations will strive? What new methods and new facts in the wide and rich field of mathematical thought will the new centuries disclose?”

One of Hilbert’s problems, known as Hilbert’s 10th problem, concerns the solutions of Diophantine equations. ”Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.”

Hilbert is not concerned with finding solutions to the equation, his question is more in the direction of deciding if there are any solutions at all. The French mathematician Poincaré also shows interest in this type of problems, and in 1901 he formulates a conjecture concerning rational solutions of elliptic curves, i.e. the solution set of a qubic equation. His claim is that the set of rational points on an elliptic curve forms a finitely generated abelian group, a claim the American-born British mathematician Louis Mordell should prove some twenty years later.

In the meantime, the number theorists published several results concerning solutions of Diophantine equations. In 1909, the Norwegian mathematician Axel Thue showed (among other things) that the equation $y^3 - 2x^2 = -1$ has only finitely many integer solutions. It was later proved that the equation has exactly one solution, given by $x = 78$ and $y = 23$.

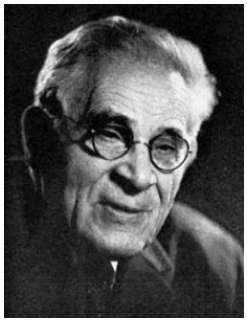
Axel Thue, 1863-1922
(Photo: Wikipedia)

Thue's more general result is known as Thue's theorem. It states that if $f(x,y)$ is a homogeneous polynomial with integer coefficients, irreducible over the rational numbers and of degree ≥ 3, then the equation $f(x,y) = k$ will have only finitely many integer solutions for an arbitrary choice of the integer k. Mordell himself showed already in 1913 that the equation

$$y^2 = x^3 + k$$

where k is an integer, has only a finite number of integer solutions.

The main result of Mordell's 1922 paper is what has since been called Mordell's theorem: The group $E(\mathbb{Q})$ of $\mathbb{Q}$-points on an elliptic curve E is finitely generated. This result came as an answer to the problem formulated by Poincaré in 1901.



Louis Mordell, 1888-1972
(Photo: The University of Manchester)

Mordell's theorem refers to the fact that an elliptic curve, typically defined as the solution set of an equation of the form

$$y^2 = x^3 + px + q$$

has an additional structure as an abelian group. The group law is often called the chord and tangent rule, since the construction is given by a purely geometric recipe, involving chords and tangents. Mordell proves his result by the classical method of infinite descent. If there are infinitely many solutions, they can all be traced back by the chord and tangent rule to only finitely many generating solutions. Mordell also shows the result which is crucial for his theorem, namely that the sum of two rational points on the elliptic curve again is a rational point.

Based on the shape of the solution set of a general equation of degree 3, elliptic curves are also referred to as curves of genus 1. Curves of higher genuses are defined by equations of higher degree, and the solution sets of these equations are also increasingly more complicated.

Mordell's conjecture, also presented in his 1922 paper "On the Rational Solutions of the Indeterminate Equations of the Third and Fourth Degree" claims that the set of rational points on curves of genus ≥ 2 is finite. This is not true for elliptic curves. Finitely generated is not the same as finite, due to the fact that rational points on the curve might have infinite order.

The Norwegian mathematician Trygve Nagell was a student of Axel Thue. He found a criterion for a rational point on an elliptic curve to be of finite order. The result is known as the Nagell-Lutz Theorem, honouring Nagell and Elisabeth Lutz. Elisabeth Lutz was a French mathematician who discovered the theorem independently of Nagell. The Nagell-Lutz Theorem describes rational points of finite order on elliptic curves over the integers: Assume that the equation

Trygve Nagell, 1895-1988
(Photo: Wikipedia)

$$y^2 = x^3 + px + q, \quad p, q \in \mathbb{Z}$$

defines a non-singular elliptic curve E with discriminant

$$\Delta = -4p^3 - 27q^2 \neq 0$$

If $P = (x,y)$ is a rational point of finite order on E, then x and y are integers and either $y = 0$, in which case P has order 2, or else y divides Δ, which immediately implies that y^2 divides Δ.

Let E be the elliptic curve given by

$$y^2 = x^3 - 4x + 9, \quad \Delta = -256 + 2187 = 1931$$

It is easily seen that $P = (2,3)$ is a rational point on E. Obviously 3 is not a factor of 1931 and P has therefore infinite order by the Nagell-Lutz theorem.

As another example, the equation $y^2 = x^3 - x$ has only 4 rational points, including the additive identity 0 at infinity; $P = (1,0)$, $Q = (-1,0)$, $P + Q = (0,0)$, and $2P = 2Q = 0$, i.e. $E(\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. Together the two examples illustrate the fact that elliptic curves may or may not have infinitely many rational points.

Axel Thue and Jean Mordell were both number theorists.Their methods are either purely arithmetic or more approximative. After Faltings and Wiles, we have realized that the solutions to number theory problems are likely to be found in other fields of mathematics than number theory itself.