Analytic and arithmetic solutions of algebraic equations

Jean-Pierre Demailly

Institut Fourier, Université Grenoble Alpes & Académie des Sciences de Paris

SISSA Colloquium

40^{th} anniversary of the School Foundation

Trieste, October 3, 2018

Solutions of algebraic equations (degrees 2 and 3)

Solution of quadratic equations (Babylonians): $ax^2 + bx + c = 0$

$$x_k = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}, \quad k = 1, 2$$

Solutions of algebraic equations (degrees 2 and 3)

Solution of quadratic equations (Babylonians): $ax^2 + bx + c = 0$

$$x_k = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}, \quad k = 1, 2$$

Solution of cubic equations (Niccolo Tartaglia, Gerolamo Cardano):

$x^3 + px + q = 0$ has 3 complex solutions $x_k = j^k u + \bar{j}^k v$, $k = 1, 2, 3$

$$\text{where } j = -\frac{1}{2} + i\frac{\sqrt{3}}{2}, \; u = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}, \quad v = -\frac{p/3}{u}.$$

Tartaglia
$\sim$ 1535

Cardano

Solutions of algebraic equations (higher degrees)

Solution of quartic equations (Lodovico Ferrari, 1540):

The solution of $ax^4 + bx^3 + cx^2 + dx + e = 0$ can be reduced to solving consecutively one cubic and two quadratic equations.

Solutions of algebraic equations (higher degrees)

Solution of quartic equations (Lodovico Ferrari, 1540):

The solution of $ax^4 + bx^3 + cx^2 + dx + e = 0$ can be reduced to solving consecutively one cubic and two quadratic equations.

However, Paolo Ruffini, Niels Abel and finally Évariste Galois ($\sim$ 1831) show the impossibility of solving equations of degree ≥ 5 by using only radicals.

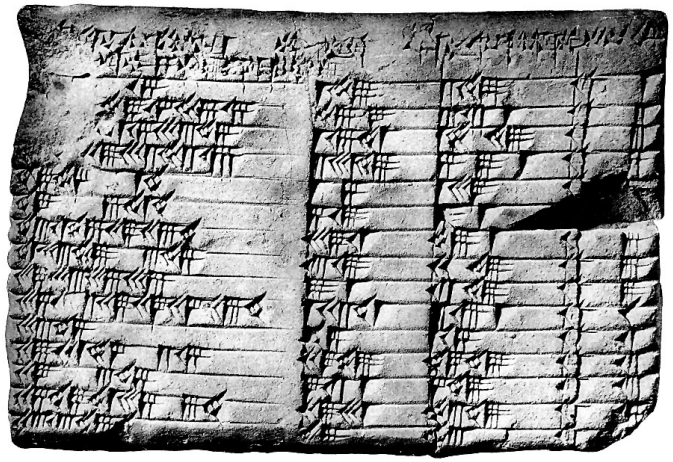
Ferrari

Galois

Galois's proof relies on the fact that the symmetric group $\mathfrak{S}_n$ of permutation of roots is not solvable for $n \geq 5$.

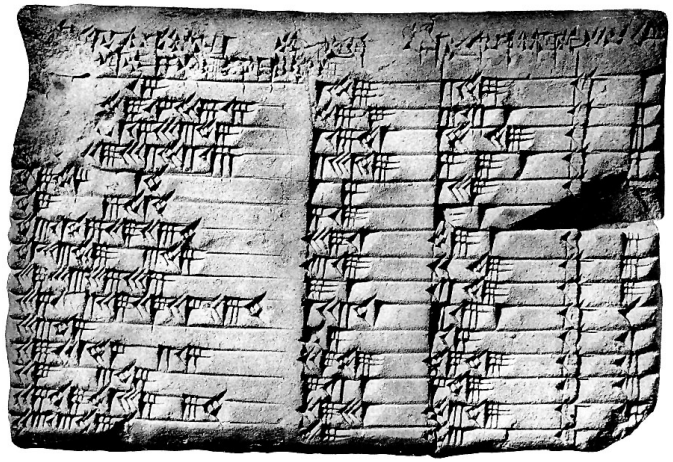
Diophantine equations

Babylonian tablet ($\sim$ 1800 BC) showing Pythagorean triples



Diophantine equations

Babylonian tablet ($\sim$ 1800 BC) showing Pythagorean triples



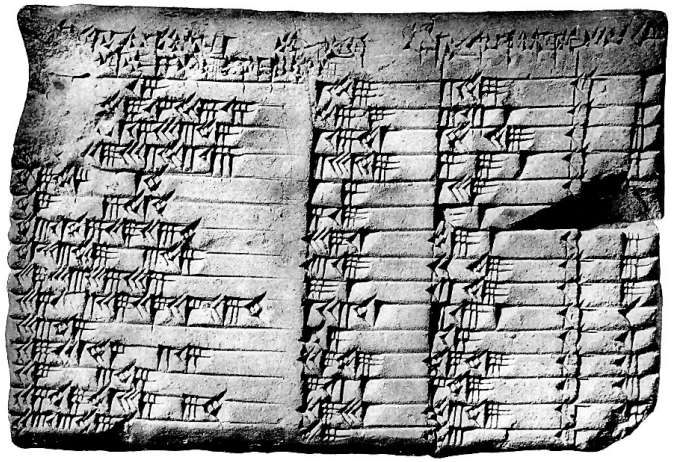
Pythagorean triples (a, b, c) are triples of positive integers such that

$$a^2 + b^2 = c^2,$$

in other words, they represent rectangular triangles.

Diophantine equations

Babylonian tablet ($\sim$ 1800 BC) showing Pythagorean triples



Pythagorean triples (a, b, c) are triples of positive integers such that

$$a^2 + b^2 = c^2,$$

in other words, they represent rectangular triangles.

The general solution attributed to Euclid is

$$a = k(p^2 - q^2), \quad b = 2kpq, \quad c = k(p^2 + q^2)$$

where $k > 0, p > q > 0$ are integers.

Interpretation of Euclid's solution

The equation $a^2 + b^2 = c^2$ is equivalent to

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1 \quad \Leftrightarrow \quad x^2 + y^2 = 1$$

by putting $x = \frac{a}{c}$, $y = \frac{b}{c}$.

Interpretation of Euclid's solution

The equation $a^2 + b^2 = c^2$ is equivalent to

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1 \quad \Leftrightarrow \quad x^2 + y^2 = 1$$

by putting $x = \frac{a}{c}$, $y = \frac{b}{c}$.Now, the solution is given by

$$x = \frac{a}{c} = \frac{p^2 - q^2}{p^2 + q^2}, \quad y = \frac{b}{c} = \frac{2pq}{p^2 + q^2}$$

which is equivalent to

$$(*) \qquad x = \frac{1 - t^2}{1 + t^2}, \quad y = \frac{2t}{1 + t^2}, \quad t = \frac{q}{p}.$$

Interpretation of Euclid's solution

The equation $a^2 + b^2 = c^2$ is equivalent to

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1 \quad \Leftrightarrow \quad x^2 + y^2 = 1$$

by putting $x = \frac{a}{c}$, $y = \frac{b}{c}$.Now, the solution is given by

$$x = \frac{a}{c} = \frac{p^2 - q^2}{p^2 + q^2}, \quad y = \frac{b}{c} = \frac{2pq}{p^2 + q^2}$$

which is equivalent to

$$(*) \qquad x = \frac{1 - t^2}{1 + t^2}, \quad y = \frac{2t}{1 + t^2}, \quad t = \frac{q}{p}.$$

Clearly, any rational value of $t \in \mathbb{Q}$ yields a rational point $(x, y) \in \mathbb{Q}^2$, which itself corresponds to a Pythagorean triple (a, b, c). The important point is that $(*)$ is a rational parametrization of the circle.

Rational curves

More generally, consider a polynomial equation $P(x, y) = 0$ with integer coefficients, and assume that there is a parametrization

$$x = \frac{R(t)}{Q(t)}, \quad y = \frac{V(t)}{U(t)}$$

as rational functions with integer coefficients, then we get infinitely many rational solutions by taking $t \in \mathbb{Q}$.

Rational curves

More generally, consider a polynomial equation $P(x, y) = 0$ with integer coefficients, and assume that there is a parametrization

$$x = \frac{R(t)}{Q(t)}, \quad y = \frac{V(t)}{U(t)}$$

as rational functions with integer coefficients, then we get infinitely many rational solutions by taking $t \in \mathbb{Q}$.

Hence, the important issue is whether the curve $C = \{P(x, y) = 0\}$. admits a rational parametrization.

Rational curves

More generally, consider a polynomial equation $P(x, y) = 0$ with integer coefficients, and assume that there is a parametrization

$$x = \frac{R(t)}{Q(t)}, \quad y = \frac{V(t)}{U(t)}$$

as rational functions with integer coefficients, then we get infinitely many rational solutions by taking $t \in \mathbb{Q}$.

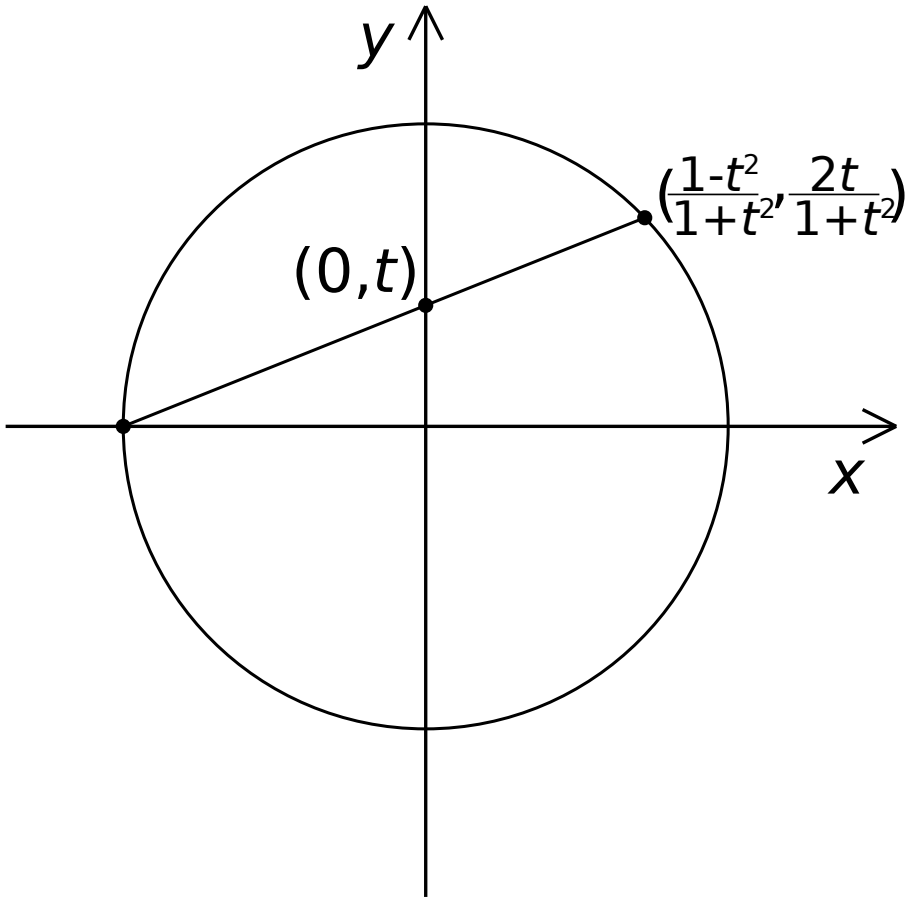
Hence, the important issue is whether the curve $C = \{P(x, y) = 0\}$. admits a rational parametrization.

It is convenient to work with complex numbers and consider more generally homogeneous polynomial equations

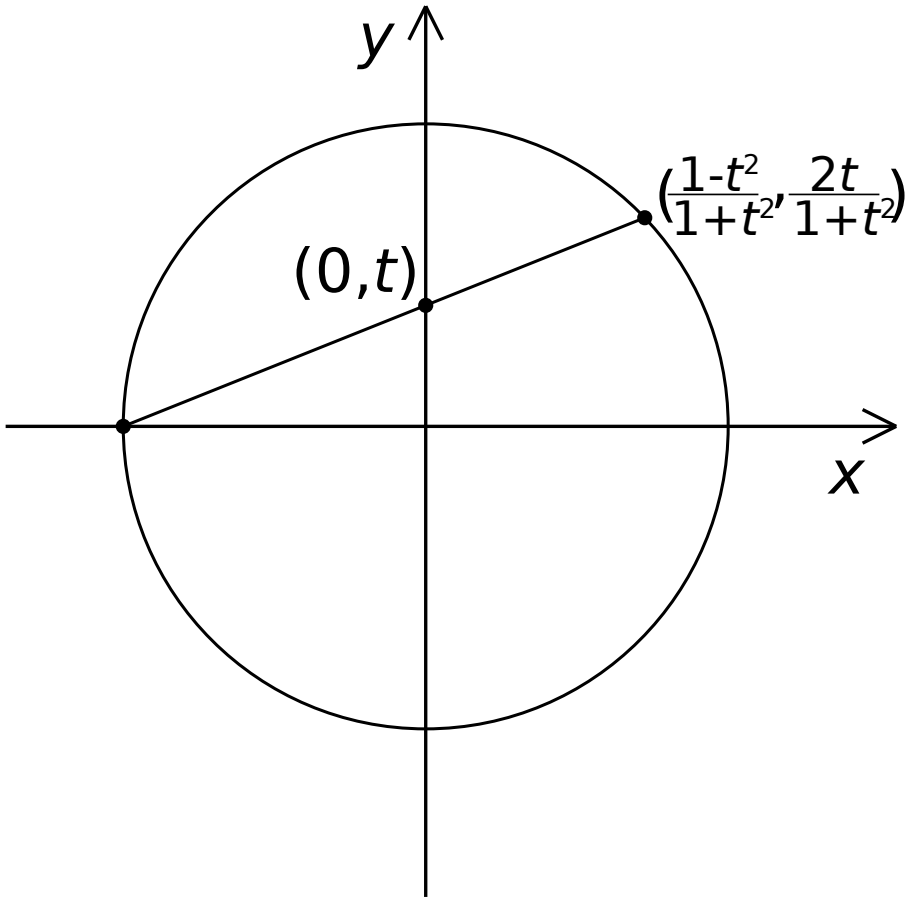
$$P(x, y, z) = 0 \quad \Leftrightarrow \quad P(x/z, y/z, 1) = 0,$$

which amounts to work in the complex projective plane of points $[x : y : z] \simeq (x/z, y/z)$, with a line $z = 0$ of "points at infinity".

Conics



Conics

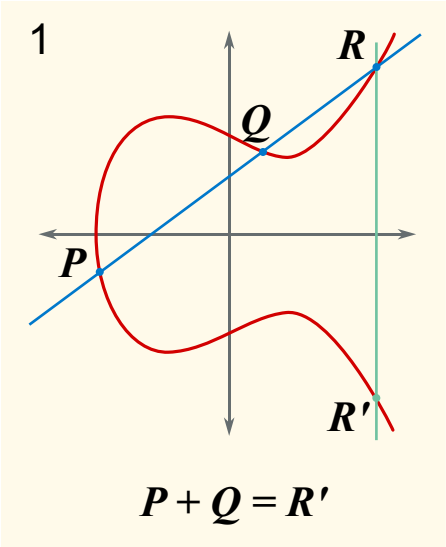


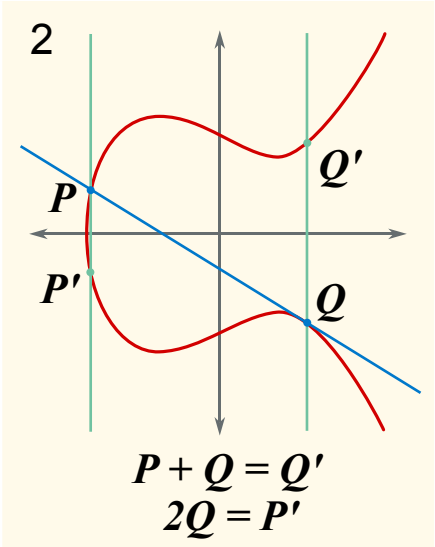
In fact, all plane conics $C = \{ax^2 + bx^2 + cxy + dx + ey + f = 0\}$ can be parametrized in that way, and if the coefficients are rational (with $C(\mathbb{Q}) \neq \emptyset$ and $C(\mathbb{R})$ not reduced to a point), then C contains infinitely many rational points.

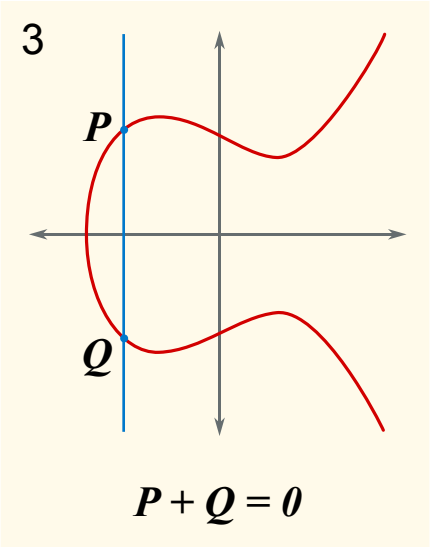
Elliptic curves

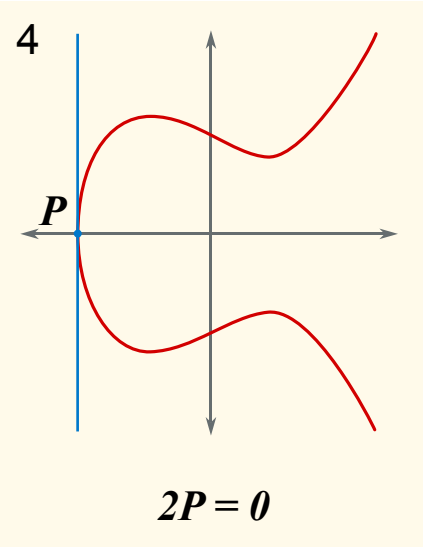
Elliptic curves can be defined by plane equations of the form

$$y^2 = x^3 + ax + b \quad \text{(below, } y^2 = x^3 - x + 1 \text{ is shown)}$$





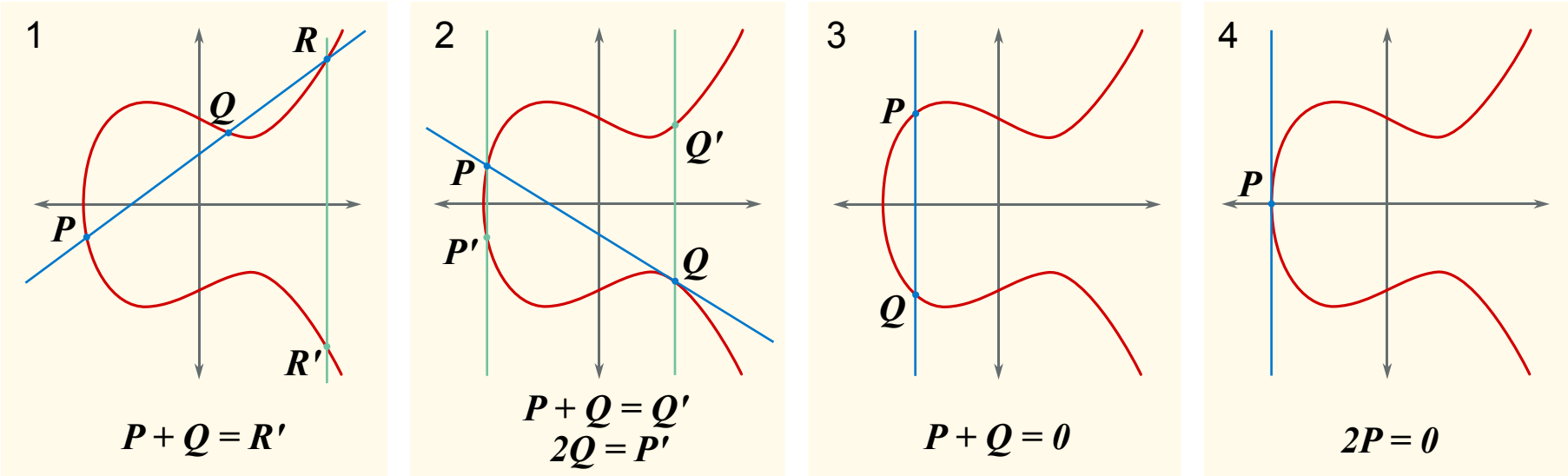




Elliptic curves

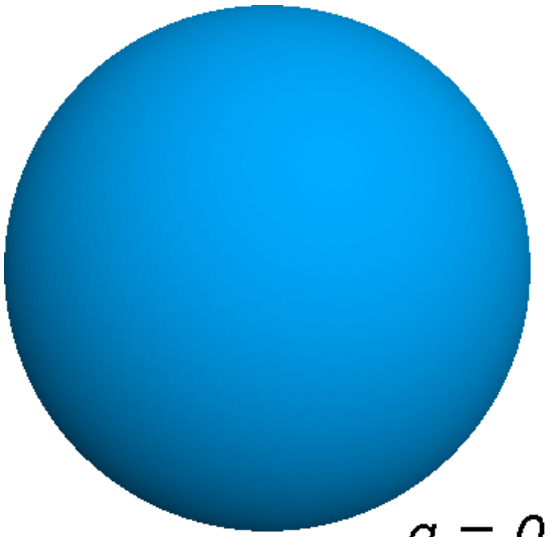
Elliptic curves can be defined by plane equations of the form

$$y^2 = x^3 + ax + b \quad \text{(below, } y^2 = x^3 - x + 1 \text{ is shown)}$$



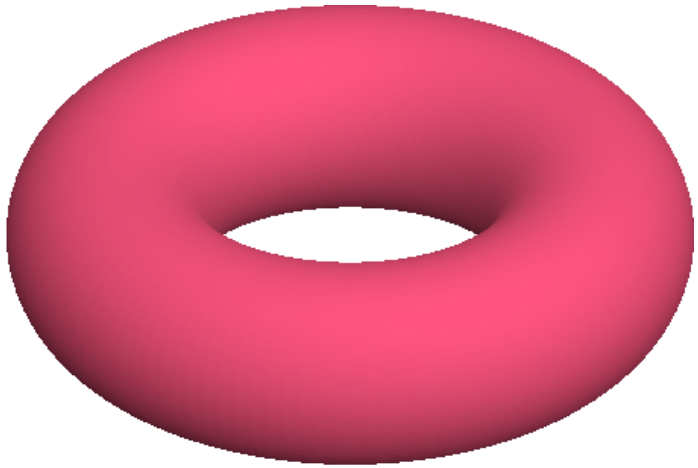
A fundamental property is that are isomorphic to an additive group $(\mathbb{C}/\Lambda, +)$ (2-torus) where Λ is a lattice, and they can be parametrized as $(x, y) = (\wp(t), \wp'(t))$ where $\wp$ is the Weierstrass $\wp$ function (a transcendental, Λ-periodic, meromorphic function of $t \in \mathbb{C}$).

Classification of curves ("Riemann surfaces")



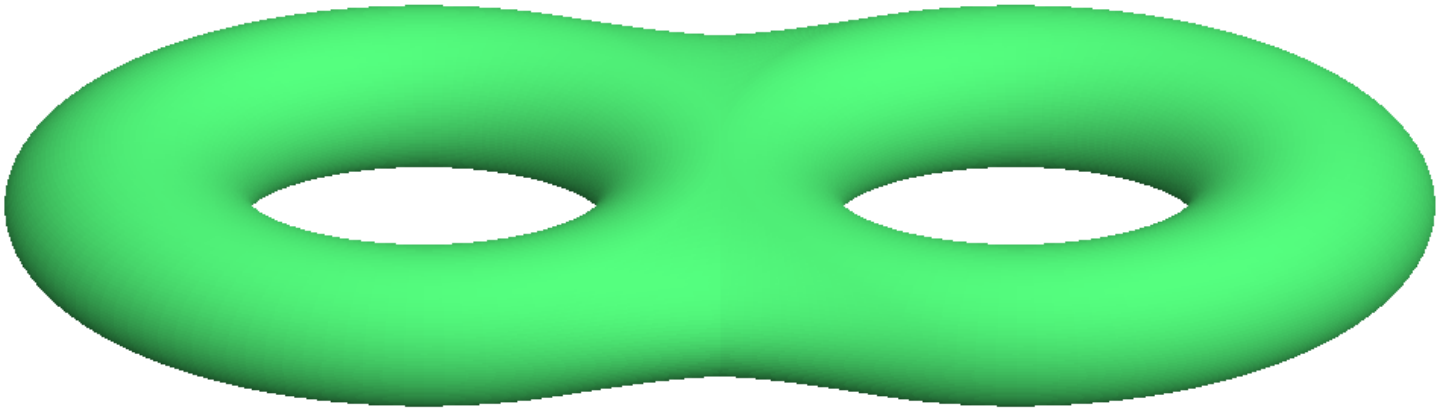
$g = 0\,,\ K_X < 0$

(positive curvature)



$g = 1\,,\ K_X = 0$

(zero curvature)



$g > 1\,,\ K_X > 0$

(negative curvature)

Over $\mathbb{C}$, curves are surfaces!

Rational points on curves

L. Mordell

G. Faltings

Gerd Faltings, Fields medal 1986 for the solution of a conjecture by Louis Mordell (1922):

Theorem (Faltings, 1983)

Let C be a smooth curve of genus $g \geq 2$ in the complex projective plane, defined as $\{P(x, y, z) = 0\}$ for some homogeneous polynomial $P(x, y, z) \in \mathbb{Q}[x, y, z]$. Then the curve C contains finitely many rational points $[x : y : z]$, i.e. $x, y, z \in \mathbb{Q}$.

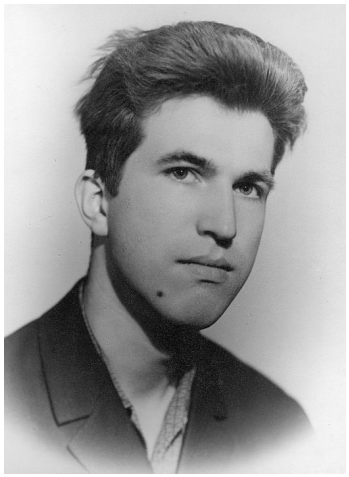
General Diophantine equations

General diophantine equations $P_j(x_0, x_1, \ldots, x_n) = 0$, $1 \leq j \leq m$ are much harder.

General Diophantine equations

General diophantine equations $P_j(x_0, x_1, \ldots, x_n) = 0$, $1 \leq j \leq m$ are much harder.

Hilbert

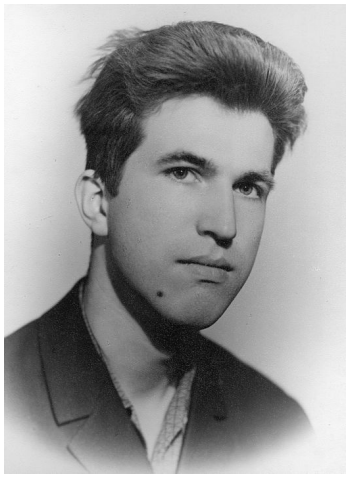


Matiyasevich

General Diophantine equations

General diophantine equations $P_j(x_0, x_1, \ldots, x_n) = 0$, $1 \leq j \leq m$ are much harder.

Hilbert



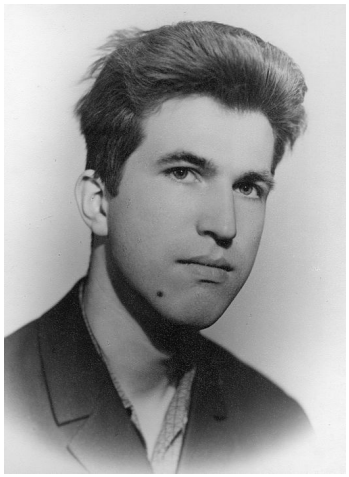
Matiyasevich

Yuri Matiyasevich became famous for proving in 1970 the inexistence of an algorithm deciding whether arbitrary Diophantine equations have solutions (Hilbert's 10^{th} problem from the 1900 Paris congress); some equations may be undecidable.

General Diophantine equations

General diophantine equations $P_j(x_0, x_1, \ldots, x_n) = 0$, $1 \leq j \leq m$ are much harder.

Hilbert

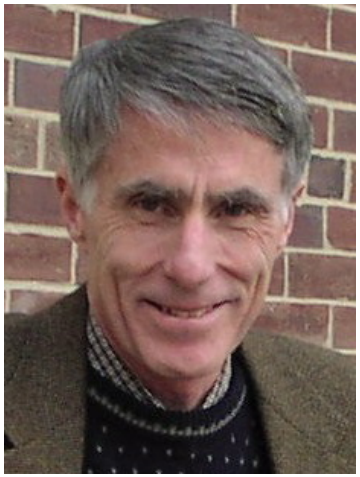


Matiyasevich

Yuri Matiyasevich became famous for proving in 1970 the inexistence of an algorithm deciding whether arbitrary Diophantine equations have solutions (Hilbert's 10^{th} problem from the 1900 Paris congress); some equations may be undecidable.

In fact, Diophantine equations can encompass many mathematical algorithms, e.g. there exists a polynomial $P \in \mathbb{Z}[X_1, \ldots, X_{26}]$ whose set of positive values is the set of prime numbers !

(Non) existence of rational & elliptic curves



H. Clemens

C. Voisin

Theorem (Herb Clemens $\sim$ 1986, Claire Voisin $\sim$ 1996)

Let $X = \{P(z_0, \ldots, z_{n+1}) = 0\}$ be a generic n-dimensional algebraic hypersurface in complex projective space (i.e. with general enough "random" coefficients) of degree $d \geq 2n + 1$, $n \geq 2$. Then X does not contain rational or elliptic curves.

In other words, there are no entire curves $f : \mathbb{C} \to X$ solving the equation $P(f(t)) = 0$, where f is either rational or a Weierstrass type transcendental function.

The Kobayashi conjecture

S. Kobayashi

Conjecture (Shoshichi Kobayashi $\sim$ 1970)

Let $X = \{P(z_0, \ldots, z_{n+1}) = 0\}$ be a generic n-dimensional algebraic hypersurface in complex projective space (i.e. with general enough "random" coefficients) of sufficiently large degree $d \geq d_n$. Then X contains no entire holomorphic curve $f : \mathbb{C} \to X$.

The Kobayashi conjecture

S. Kobayashi

Conjecture (Shoshichi Kobayashi $\sim$ 1970)

Let $X = \{P(z_0, \ldots, z_{n+1}) = 0\}$ be a generic n-dimensional algebraic hypersurface in complex projective space (i.e. with general enough "random" coefficients) of sufficiently large degree $d \geq d_n$. Then X contains no entire holomorphic curve $f : \mathbb{C} \to X$.

Definition

X is said to be Kobayashi hyperbolic if it contains no entire holomorphic curve $f : \mathbb{C} \to X$.

Solution of Kobayashi conjecture (Brotbek 2016)

Theorem (Brotbek 2016)

The Kobayashi conjecture holds true for $d_n \gg 1$ (non explicit), i.e. a generic polynomial equation $P(z) = 0$ of degree $d \geq d_n$ contains no entire analytic solution $z = f(t)$, $t \in \mathbb{C}$.

Solution of Kobayashi conjecture (Brotbek 2016)

Theorem (Brotbek 2016)

The Kobayashi conjecture holds true for $d_n \gg 1$ (non explicit), i.e. a generic polynomial equation $P(z) = 0$ of degree $d \geq d_n$ contains no entire analytic solution $z = f(t)$, $t \in \mathbb{C}$.

My PhD student Ya Deng found a way to make d_n explicit.

Solution of Kobayashi conjecture (Brotbek 2016)

Theorem (Brotbek 2016)

The Kobayashi conjecture holds true for $d_n \gg 1$ (non explicit), i.e. a generic polynomial equation $P(z) = 0$ of degree $d \geq d_n$ contains no entire analytic solution $z = f(t)$, $t \in \mathbb{C}$.

My PhD student Ya Deng found a way to make d_n explicit.

Theorem (simpler proof, Demailly 2018)

The Kobayashi conjecture holds for $d \geq d_n = \lfloor (en)^{2n+2}/3 \rfloor$.

Solution of Kobayashi conjecture (Brotbek 2016)

Theorem (Brotbek 2016)

The Kobayashi conjecture holds true for $d_n \gg 1$ (non explicit), i.e. a generic polynomial equation $P(z) = 0$ of degree $d \geq d_n$ contains no entire analytic solution $z = f(t)$, $t \in \mathbb{C}$.

My PhD student Ya Deng found a way to make d_n explicit.

Theorem (simpler proof, Demailly 2018)

The Kobayashi conjecture holds for $d \geq d_n = \lfloor (en)^{2n+2}/3 \rfloor$.

The proof is based on finding certain algebraic differential operators

$$D(f) = \sum a_{\alpha_1 \ldots \alpha_k}(f)(f')^{\alpha_1}(f'')^{\alpha_2} \ldots (f^{(k)})^{\alpha_k}$$

whose coefficients a_α vanish along some hyperplane section $H \subset X$.

Solution of Kobayashi conjecture (Brotbek 2016)

Theorem (Brotbek 2016)

The Kobayashi conjecture holds true for $d_n \gg 1$ (non explicit), i.e. a generic polynomial equation $P(z) = 0$ of degree $d \geq d_n$ contains no entire analytic solution $z = f(t)$, $t \in \mathbb{C}$.

My PhD student Ya Deng found a way to make d_n explicit.

Theorem (simpler proof, Demailly 2018)

The Kobayashi conjecture holds for $d \geq d_n = \lfloor (en)^{2n+2}/3 \rfloor$.

The proof is based on finding certain algebraic differential operators

$$D(f) = \sum a_{\alpha_1 \ldots \alpha_k}(f)(f')^{\alpha_1}(f'')^{\alpha_2} \ldots (f^{(k)})^{\alpha_k}$$

whose coefficients a_α vanish along some hyperplane section $H \subset X$.

Theorem (Green-Griffiths 1979, D– 1995, Siu-Yeung 1996)

If such a global operator D exists on X, then all entire curves $f : \mathbb{C} \to X$ must satisfy the differential equation $D(f) \equiv 0$.

Simplified proof of Kobayashi conjecture

The "simplified proof" consists of finding sufficiently many global differential operators $D(f) = 0$ in the form of Wronskians

$$W(s_0, \ldots, s_k)(f) = \begin{vmatrix} s_0(f) & s_1(f) & \ldots & s_k(f) \\ \nabla(s_0(f)) & \nabla(s_1(f)) & \ldots & \nabla(s_k(f)) \\ \vdots & & & \vdots \\ \nabla^k(s_0(f)) & \nabla^k(s_1(f)) & \ldots & \nabla^k(s_k(f)) \end{vmatrix}$$

Simplified proof of Kobayashi conjecture

The "simplified proof" consists of finding sufficiently many global differential operators $D(f) = 0$ in the form of Wronskians

$$W(s_0, \ldots, s_k)(f) = \begin{vmatrix} s_0(f) & s_1(f) & \ldots & s_k(f) \\ \nabla(s_0(f)) & \nabla(s_1(f)) & \ldots & \nabla(s_k(f)) \\ \vdots & & & \vdots \\ \nabla^k(s_0(f)) & \nabla^k(s_1(f)) & \ldots & \nabla^k(s_k(f)) \end{vmatrix}$$

In general they do not exist, but one can show that they exist on well chosen "Fermat type" hypersurfaces $\sum m_j(z)^k = 0$ where the $m_j(z) = z^{\beta_j}$ are suitable monomials.

Simplified proof of Kobayashi conjecture

The "simplified proof" consists of finding sufficiently many global differential operators $D(f) = 0$ in the form of Wronskians

$$W(s_0, \ldots, s_k)(f) = \begin{vmatrix} s_0(f) & s_1(f) & \ldots & s_k(f) \\ \nabla(s_0(f)) & \nabla(s_1(f)) & \ldots & \nabla(s_k(f)) \\ \vdots & & & \vdots \\ \nabla^k(s_0(f)) & \nabla^k(s_1(f)) & \ldots & \nabla^k(s_k(f)) \end{vmatrix}$$

In general they do not exist, but one can show that they exist on well chosen "Fermat type" hypersurfaces $\sum m_j(z)^k = 0$ where the $m_j(z) = z^{\beta_j}$ are suitable monomials.

Moreover, by using the geometric structure of jet bundles elaborated in (D–, 1995), one can show that these operators have "deformations" to generic hypersurfaces of high degree.

Green-Griffiths conjecture

M. Green

P. Griffiths

Conjecture (Mark Green & Phillip Griffiths 1979)

Let $X = \{P(z_0, \ldots, z_{n+1}) = 0\}$ be a smooth n-dimensional algebraic hypersurface in complex projective space. Assume $d = \deg P \geq n + 2$. Then X possesses an algebraic subvariety $Y = \{Q(z) = 0\}$ containg all entire curves $f : \mathbb{C} \to X$, i.e. $Q(f) = 0$.

Green-Griffiths conjecture

M. Green

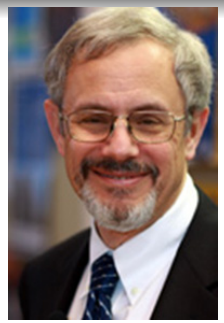
P. Griffiths

Conjecture (Mark Green & Phillip Griffiths 1979)

Let $X = \{P(z_0, \ldots, z_{n+1}) = 0\}$ be a smooth n-dimensional algebraic hypersurface in complex projective space. Assume $d = \deg P \geq n + 2$. Then X possesses an algebraic subvariety $Y = \{Q(z) = 0\}$ containg all entire curves $f : \mathbb{C} \to X$, i.e. $Q(f) = 0$.

The smallest $Y = \mathrm{GG}(X)$ is called the Green-Griffiths locus of X.

Green-Griffiths conjecture



M. Green

P. Griffiths

Conjecture (Mark Green & Phillip Griffiths 1979)

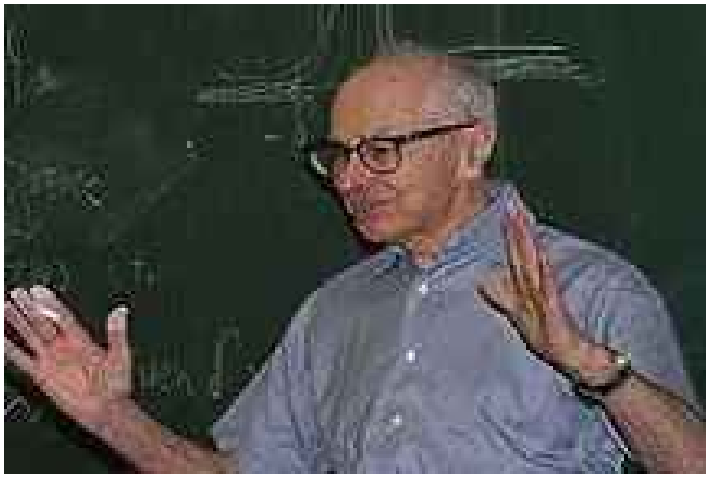
Let $X = \{P(z_0, \ldots, z_{n+1}) = 0\}$ be a smooth n-dimensional algebraic hypersurface in complex projective space. Assume $d = \deg P \geq n + 2$. Then X possesses an algebraic subvariety $Y = \{Q(z) = 0\}$ containg all entire curves $f : \mathbb{C} \to X$, i.e. $Q(f) = 0$.

The smallest $Y = \mathrm{GG}(X)$ is called the Green-Griffiths locus of X.

Theorem (Demailly 2010)

Rather than an algebraic equation $Q(f) = 0$, such entire curves $f : \mathbb{C} \to X = \{P = 0\}$, $\deg P \geq n + 2$, satisfy at least one (and in fact many) algebraic differential equations $D(f) = 0$.

Lang-Vojta program

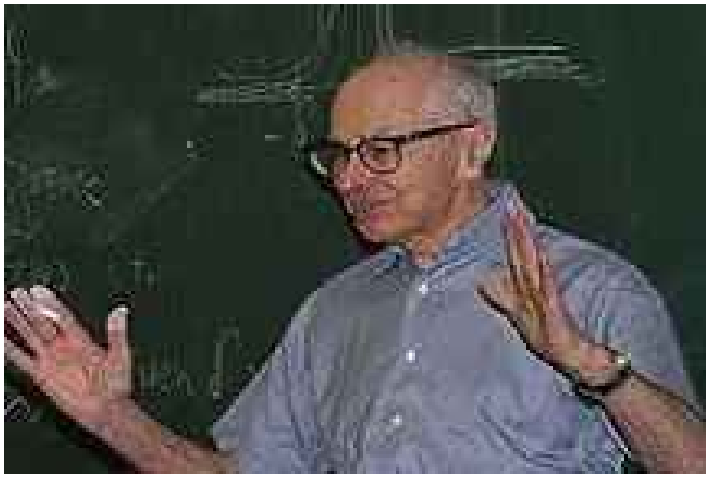


S. Lang

P. Vojta

This is a fascinating program that tries to relate the algebro-geometric properties of algebraic varieties with their arithmetic properties.

Lang-Vojta program



S. Lang

P. Vojta

This is a fascinating program that tries to relate the algebro-geometric properties of algebraic varieties with their arithmetic properties.

Lang's conjecture 1987 – very optimistic ?

For X projective defined over a number field $\mathbb{K}_0$, the Green-Griffiths locus $\mathrm{GG}(X)$ in GG conjecture equals $\mathrm{Mordell}(X) =$ smallest Y such that $X(\mathbb{K}) \setminus Y$ is finite, $\forall \mathbb{K}$ number field $\supset \mathbb{K}_0$.

The end