1, 2, 3; a, b, c; ...

Antoine Chambert-Loir

October, 22 2019

Université Paris-Diderot

Diophantine equations

Basically:

- Unknowns are integers, or rationals numbers
- Equations are given by polynomial relations between the unknowns.

Diophantine equations

Basically:

- Unknowns are integers, or rationals numbers
- Equations are given by polynomial relations between the unknowns.

Roughly, three parameters:

- The number of variables;
- The number of equations;
- The degree of the equations.

Warm-up

Diophantine equations in *one* variable are easy to solve.

Warm-up

Diophantine equations in *one* variable are easy to solve.

Theorem

Let $a_0, \ldots, a_{n-1}, a_n \in \mathbf{C}$, *with* $a_n \neq 0$. *Every root* x *of the nth degree equation:*

$$a_n x^n + \cdots + a_1 x + a_0 = 0$$

satisfies

$$|x| \leqslant \sup\left(1, \frac{|a_0| + \cdots + |a_{n-1}|}{|a_n|}\right).$$

Warm-up

Diophantine equations in *one* variable are easy to solve.

Theorem

Let $a_0, \ldots, a_{n-1}, a_n \in \mathbf{C}$*, with* $a_n \neq 0$*. Every root* x *of the nth degree equation:*

$$a_n x^n + \cdots + a_1 x + a_0 = 0$$

satisfies

$$|x| \leqslant \sup\left(1, \frac{|a_0| + \cdots + |a_{n-1}|}{|a_n|}\right).$$

If we seek for integer solutions, it then suffices to try one by one all integers in the interval that is described by the theorem.

Geometry of diophantine equations

Equations of degree 1

An old problem: (III-V^e century C.E):

Equations of degree 1

An old problem: (III-V^{e} century C.E):

> 有物不知其數，三三數之剩二，五五數之剩三，七七數之剩二。問物几何？

An old problem: (III-V^e century C.E):

> 有物不知其數，三三數之剩二，五五數之剩三，七七數之剩二。問物几何？

That means:

> *A number of things is unknown. If one counts them by three, there remains 2; if one conts them by five, there remains 3; if one counts them by seven, there remains 2. Find this number of things.*

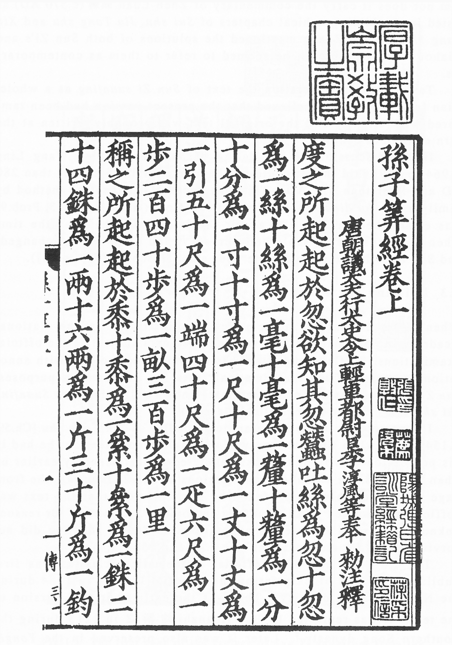
An old problem: (III-V^{e} century C.E):

> 有物不知其數，三三數之剩二，五五數之剩三，七七數之剩二。問物几何？

That means:

> *A number of things is unknown. If one counts them by three, there remains 2; if one conts them by five, there remains 3; if one counts them by seven, there remains 2. Find this number of things.*

This “Chinese problem” is due to Sūnzǐ, and was published in the Sūnzǐ Suàngjīng 孫子算經, *The Mathematical Classic of Master Sun*


孫子筭經卷上
唐朝議大夫行太史令上輕車都尉臣李淳風等奉 勑注釋
度之所起起於忽欲知其忽蠶吐絲爲忽十忽
爲一絲十絲爲一毫十毫爲一氂十氂爲一分
十分爲一寸十寸爲一尺十尺爲一丈十丈爲
一引五十尺爲一端四十尺爲一疋六尺爲一
步二百四十步爲一畝三百步爲一里
稱之所起起於黍十黍爲一絫十絫爲一銖二
十四銖爲一兩十六兩爲一斤三十斤爲一鈞

Sūnzǐ Suàngjīng, reproduction of a page from a Qing dynasty edition

Source: *Wikipedia*

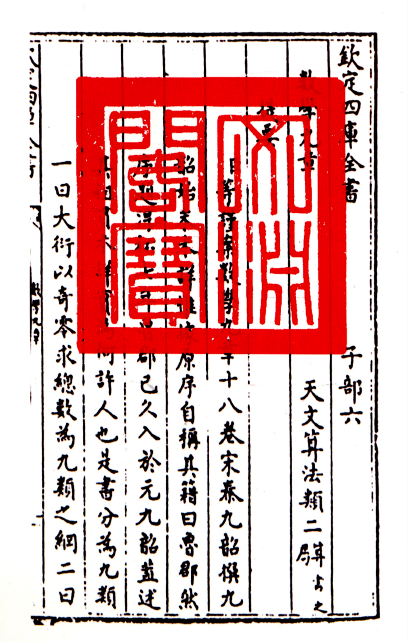
Such exercises were then reproduced in other manuals, such as the

Shùshū Jiǔzhāng —數書九章,
Mathematical treatise in nine sections, 1247,

itself included in the

Sìkù quánshū —四庫全書,
Complete Library of the Four Treasuries, xixth c.,

a kind of encyclopaedia commissionned by the Qing emperors to attest their supremacy over the former Ming encyclopaedia (ca. 1403)



A Mathematical Book in Nine Chapters
(數書九章, Shùshū Jiǔzhāng)
reproduction of the Sìkù Quánshū 四庫全書 (1847)

Source: *Wikipedia*

有物不知其數，三三數之剩二，五五數之剩三，七七數之剩二。問物几何？

> 有物不知其數，三三數之剩二，五五數之剩三，七七數之剩二。問物几何？

That is,

> *A number of things is unknown. If one counts them by three, there remains 2; if one conts them by five, there remains 3; if one counts them by seven, there remains 2. Find this number of things.*

Le problème chinois

> 有物不知其數，三三數之剩二，五五數之剩三，七七數之剩二。問物几何？

That is,

> *A number of things is unknown. If one counts them by three, there remains 2; if one conts them by five, there remains 3; if one counts them by seven, there remains 2. Find this number of things.*

Or, again, solve

$$n = 3x + 2 = 5y + 3 = 7z + 2,$$

in the main unknown n.

The "Chinese theorem" teaches us that the smallest solution is $n = 23$, and that all other solutions are obtained by adding a multiple of $105 = 3 \times 5 \times 7$.

Equations of degree 2

Πρόβλημα,

ὅπερ Ἀρχιμήδης ἐν ἐπιγράμμασιν εὑρὼν τοῖς ἐν Ἀλεξανδρείᾳ περὶ ταῦτα πραγματευομένοις ζητεῖν ἀπέστειλεν ἐν τῇ πρὸς Ἐρατοσθένην τὸν Κυρηναῖον ἐπιστολῇ.

Πληθὺν Ἠελίοιο βοῶν, ὦ ξεῖνε, μέτρησον
φροντίδ' ἐπιστήσας, εἰ μετέχεις σοφίης,
πόσση ἄρ' ἐν πεδίοις Σικελῆς ποτ' ἐβόσκετο νήσου
Θρινακίης τετραχῇ στίφεα δασσαμένη
χροιὴν ἀλλάσσοντα· τὸ μὲν λευκοῖο γάλακτος,
κυανέῳ δ' ἕτερον χρώματι λαμπόμενον,
ἄλλο γε μὲν ξανθόν, τὸ δὲ ποικίλον. ἐν δὲ ἑκάστῳ
στίφει ἔσαν ταῦροι πλήθεσι βριθόμενοι
συμμετρίης τοιῆσδε τετευχότες· ἀργότριχας μὲν
κυανέων ταύρων ἡμίσει ἠδὲ τρίτῳ
καὶ ξανθοῖς σύμπασιν ἴσους, ὦ ξεῖνε, νόησον,

Πρόβλημα,

ὅπερ Ἀρχιμήδης ἐν ἐπιγράμμασιν εὑρὼν τοῖς ἐν Ἀλεξανδρείᾳ περὶ ταῦτα πραγματευομένοις ζητεῖν ἀπέστειλεν ἐν τῇ πρὸς Ἐρατοσθένην τὸν Κυρηναῖον ἐπιστολῇ.

Πληθὺν Ἠελίοιο βοῶν, ὦ ξεῖνε, μέτρησον
φροντίδ᾽ ἐπιστήσας, εἰ μετέχεις σοφίης,
πόσση ἄρ᾽ ἐν πεδίοις Σικελῆς ποτ᾽ ἐβόσκετο νήσου
Θρινακίης τετραχῇ στίφεα δασσαμένη
χροιὴν ἀλλάσσοντα· τὸ μὲν λευκοῖο γάλακτος,
κυανέῳ δ᾽ ἕτερον χρώματι λαμπόμενον,
ἄλλο γε μὲν ξανθόν, τὸ δὲ ποικίλον. ἐν δὲ ἑκάστῳ
στίφει ἔσαν ταῦροι πλήθεσι βριθόμενοι
συμμετρίης τοιῆσδε τετευχότες· ἀργότριχας μέν
κυανέων ταύρων ἡμίσει ἠδὲ τρίτῳ
καὶ ξανθοῖς σύμπασιν ἴσους, ὦ ξεῖνε, νόησον,
αὐτὰρ κυανέους τῷ τετράτῳ τε μέρει
μικτοχρόων καὶ πέμπτῳ, ἔτι ξανθοῖσί τε πᾶσιν
τοὺς δ᾽ ὑπολειπομένους ποικιλόχρωτας ἄθρει
ἀργεννῶν ταύρων ἕκτῳ μέρει ἑβδομάτῳ τε
καὶ ξανθοῖς αὖτις πᾶσιν ἰσαζομένους.
θηλείαισι δὲ βουσὶ τάδ᾽ ἔπλετο· λευκότριχες μέν
ἦσαν συμπάσης κυανέης ἀγέλης
τῷ τριτάτῳ τε μέρει καὶ τετράτῳ ἀτρεκὲς ἶσαι·
αὐτὰρ κυάνεαι τῷ τετράτῳ τε πάλιν
μικτοχρόων καὶ πέμπτῳ ὁμοῦ μέρει ἰσάζοντο
σὺν ταύροις· πάσης δ᾽ εἰς νομὸν ἐρχομένης
ξανθοτρίχων ἀγέλης πέμπτῳ μέρει ἠδὲ καὶ ἕκτῳ
ποικίλαι ἰσάριθμον πλῆθος ἔχον τετραχῇ.
ξανθαὶ δ᾽ ἠριθμεῦντο μέρους τρίτου ἡμίσει ἶσαι
ἀργεννῆς ἀγέλης ἑβδομάτῳ τε μέρει.
ξεῖνε, σὺ δ᾽ Ἠελίοιο βοῶν πόσαι ἀτρεκὲς εἰπών,
χωρὶς μὲν ταύρων ζατρεφέων ἀριθμόν,
χωρὶς δ᾽ αὖ θήλειαι ὅσαι κατὰ χρῶμα ἕκασται,
οὐκ ἄιδρίς κε λέγοι᾽ οὐδ᾽ ἀριθμῶν ἀδαής,
οὐ μὴν πώ γε σοφοῖς ἐναρίθμιος. ἀλλ᾽ ἴθι φράζευ
καὶ τάδε πάντα βοῶν Ἠελίοιο πάθη.
ἀργότριχες ταῦροι μὲν ἐπεὶ μιξαίατο πληθύν
κυανέοις, ἵσταντ᾽ ἔμπεδον ἰσόμετροι
εἰς βάθος εἰς εὖρός τε, τὰ δ᾽ αὖ περιμήκεα πάντῃ
πίμπλαντο πλίνθου Θρινακίης πεδία.
ξανθοὶ δ᾽ αὖτ᾽ εἰς ἓν καὶ ποικίλοι ἀθροισθέντες
ἵσταντ᾽ ἀμβολάδην ἐξ ἑνὸς ἀρχόμενοι
σχῆμα τελειοῦντες τὸ τρικράσπεδον οὔτε προσόντων
ἀλλοχρόων ταύρων οὔτ᾽ ἐπιλειπομένων.
ταῦτα συνεξευρὼν καὶ ἐνὶ πραπίδεσσιν ἀθροίσας
καὶ πληθέων ἀποδοὺς, ὦ ξένε, πάντα μέτρα
ἔρχεο κυδιόων νικηφόρος, ἴσθι τε πάντως
κεκριμένος ταύτῃ ὄμπνιος ἐν σοφίῃ.

Archimedes's cattle problem
Archimedis Opera omnia, cum commentariis Eutocii
Edited by J. L. Heiberg
B. G. Teubner, Leibzig, Volume 2 (1881), pp. 448–450

The Brahmagupta (Pell–Fermat) equation

If n is a (non-square) parameter, find the solutions in rational integers to the equation

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

The Brahmagupta (Pell–Fermat) equation

If n is a (non-square) parameter, find the solutions in rational integers to the equation

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

Example: $x^2 - 2y^2 = 1$. Solutions $(3, 2)$, $(17, 12)$,...

The Brahmagupta (Pell–Fermat) equation

If n is a (non-square) parameter, find the solutions in rational integers to the equation

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

Example: $x^2 - 2y^2 = 1$. Solutions $(3, 2)$, $(17, 12)$,...

In Archimedes's problem: $n = 4 \times 609 \times 7766 \times 4657^2$...

Solving the Brahamagupta equation

Brahmagupta (628 C.E.): if (x, y) and (x', y') are solutions, one may build a third one (x'', y'') by the formula:

$$x'' = xx' + nyy', \quad y'' = xy' + x'y.$$

Solving the Brahamagupta equation

Brahmagupta (628 C.E.): if (x, y) and (x', y') are solutions, one may build a third one (x'', y'') by the formula:

$$x'' = xx' + nyy', \quad y'' = xy' + x'y.$$

All solutions (more or less) are obtained from a minimal one.

Solving the Brahamagupta equation

Brahmagupta (628 C.E.): if (x, y) and (x', y') are solutions, one may build a third one (x'', y'') by the formula:

$$x'' = xx' + nyy', \quad y'' = xy' + x'y.$$

All solutions (more or less) are obtained from a minimal one.

Modern explanation :

$$x^2 - ny^2 = (x + \sqrt{n}y)(x - \sqrt{n}y),$$

is the *norm* of the quadratic number $x + \sqrt{n}y$; it is multiplicative and one has

$$(x + \sqrt{n}y)(x' + \sqrt{n}y') = (xx' + nyy') + \sqrt{n}(xy' + x'y).$$

The Pythagoras equation

Solving the equation

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

The Pythagoras equation

Solving the equation

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

Only integer solutions: $(\pm 1, 0)$, $(0, \pm 1)$.

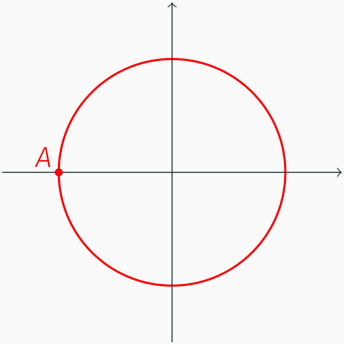
The Pythagoras equation

Solving the equation

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

Only integer solutions: $(\pm 1, 0)$, $(0, \pm 1)$.

Rational solutions?



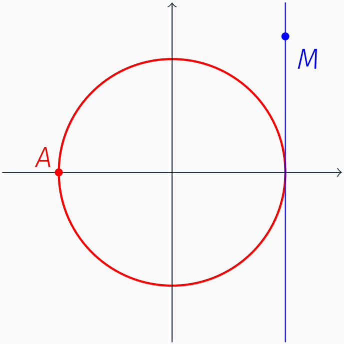
The Pythagoras equation

Solving the equation

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

Only integer solutions: $(\pm 1, 0)$, $(0, \pm 1)$.

Rational solutions?



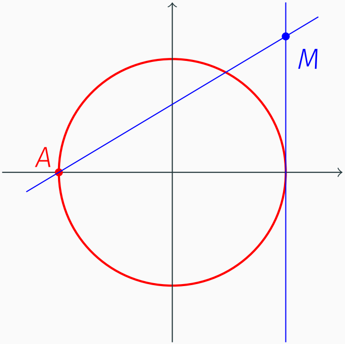
The Pythagoras equation

Solving the equation

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

Only integer solutions: $(\pm 1, 0)$, $(0, \pm 1)$.

Rational solutions?



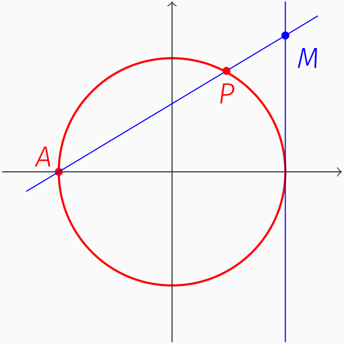
The Pythagoras equation

Solving the equation

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

Only integer solutions: $(\pm 1, 0)$, $(0, \pm 1)$.

Rational solutions?



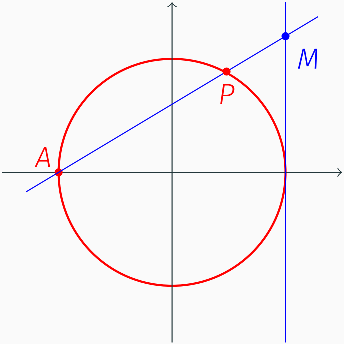
The Pythagoras equation

Solving the equation

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

Only integer solutions: $(\pm 1, 0)$, $(0, \pm 1)$.

Rational solutions?



If M has coordinates $(1, t)$, then P has coordinates (x, y) with

$$\begin{cases} x = \dfrac{1 - t^2}{1 + t^2} \\ y = \dfrac{2t}{1 + t^2} \end{cases}$$

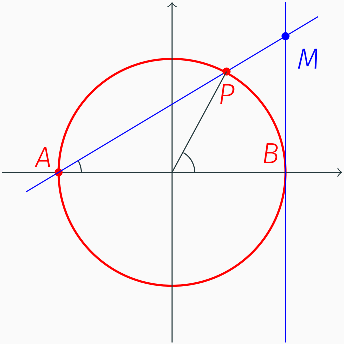
The Pythagoras equation

Solving the equation

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

Only integer solutions: $(\pm 1, 0)$, $(0, \pm 1)$.

Rational solutions?



If M has coordinates $(1, t)$, then P has coordinates (x, y) with

$$\begin{cases} x = \dfrac{1-t^2}{1+t^2} \\ y = \dfrac{2t}{1+t^2} \end{cases}$$

$t = \arctan(\widehat{BAP}) = \arctan(\widehat{BOP}/2)$

Rational parameterizing of conics

The procedure explained for the circle works for every *conic*
(given by a degree 2 equation in two variables)
provided there exists at least one solution in rational numbers.

Rational parameterizing of conics

The procedure explained for the circle works for every *conic* (given by a degree 2 equation in two variables) *provided* there exists at least one solution in rational numbers.

Examples:

- $x^2 + y^2 = -1$ — sign issue.
- $x^2 + y^2 = 3$ — congruence modulo 4.

Rational parameterizing of conics

The procedure explained for the circle works for every *conic* (given by a degree 2 equation in two variables) *provided* there exists at least one solution in rational numbers.

Examples:

- $x^2 + y^2 = -1$ — sign issue.
- $x^2 + y^2 = 3$ — congruence modulo 4.

Theorem (Hasse, 1921)

If there is no sign issue, no congruence issue, then there is a solution in rational numbers.

Rational parameterizing of conics

The procedure explained for the circle works for every *conic* (given by a degree 2 equation in two variables) *provided* there exists at least one solution in rational numbers.

Examples:

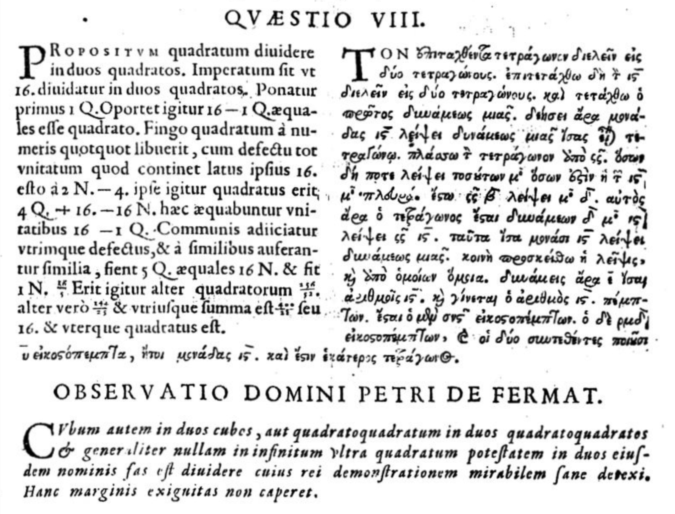
- $x^2 + y^2 = -1$ — sign issue.
- $x^2 + y^2 = 3$ — congruence modulo 4.

Theorem (Hasse, 1921)

If there is no sign issue, no congruence issue, then there is a solution in rational numbers.

More generally: *If a quadratic form $q(x, y, z, \dots)$ with coefficients in* $\mathbf{Q}$ *has non-trivial solutions in all p-adic fields* $\mathbf{Q}_p$*, as well as in* $\mathbf{R}$*, then it has a non-trivial solution*

Equations of degree 3 or more



QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum sit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 − 1 Q. æquales esse quadrato. Fingo quadratum à numeris quotquot libuerit, cum defectu tot vnitatum quod continet latus ipsius 16. esto à 2 N. − 4. ipse igitur quadratus erit 4 Q. + 16. − 16 N. hæc æquabuntur vnitatibus 16 − 1 Q. Communis adiiciatur vtrimque defectus, & à similibus auferantur similia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{16}{5}$ Erit igitur alter quadratorum $\frac{256}{25}$. alter verò $\frac{144}{25}$ & vtriusque summa est $\frac{400}{25}$ seu 16. & vterque quadratus est.

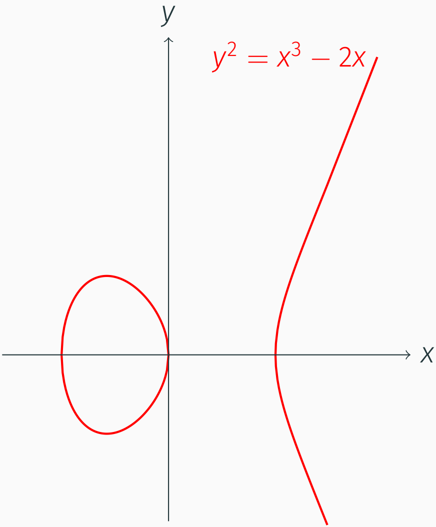
ΤΟΝ ἐπιταχθέντα τετράγωνον διελεῖν εἰς δύο τετραγώνους. ἐπιτετάχθω δὴ τὸν ιϛ διελεῖν εἰς δύο τετραγώνους. καὶ τετάχθω ὁ πρῶτος δυνάμεως μιᾶς. δεήσει ἄρα μονάδας ιϛ λείψει δυνάμεως μιᾶς ἴσας εἶναι τετραγώνῳ. πλάσσω τὸ τετράγωνον ἀπὸ ςˢ. ὅσων δή ποτε λείψει τοσούτων μ° ὅσων ἐστὶν ἡ τοῦ ιϛ μ° πλευρά. ἔστω ςˢ β λείψει μ° δ. αὐτὸς ἄρα ὁ τετράγωνος ἔσται δυνάμεων δ μ° ιϛ λείψει ςˢ ιϛ. ταῦτα ἴσα μονάσι ιϛ λείψει δυνάμεως μιᾶς. κοινὴ προσκείσθω ἡ λεῖψις, καὶ ἀπὸ ὁμοίων ὅμοια. δυνάμεις ἄρα ε ἴσαι ἀριθμοῖς ιϛ. καὶ γίνεται ὁ ἀριθμὸς ιϛ πέμπτων. ἔσται ὁ μὲν σνϛ εἰκοστοπέμπτων. ὁ δὲ ρμδ εἰκοστοπέμπτων, καὶ οἱ δύο συντεθέντες ποιοῦσι υ εἰκοστόπεμπτα, ἤτοι μονάδας ιϛ. καὶ ἔστιν ἑκάτερος τετράγωνος.

OBSERVATIO DOMINI PETRI DE FERMAT.

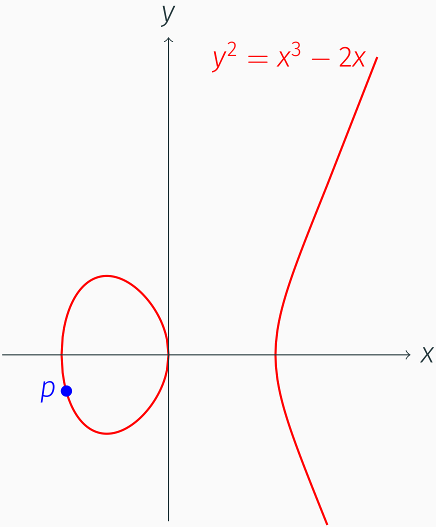
Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Diophante, *Arithmetica*. Bachet de Méziriac edition, 1670.
Source: *Wikipedia*

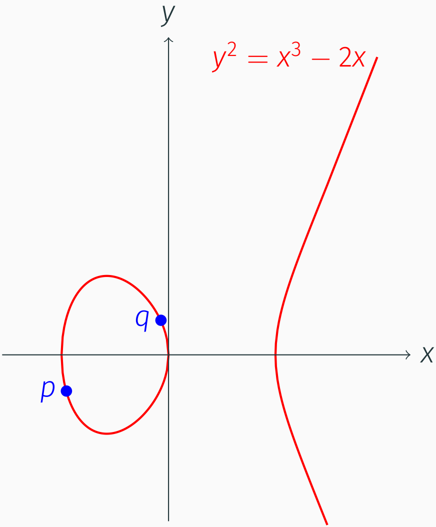
A cubic equation



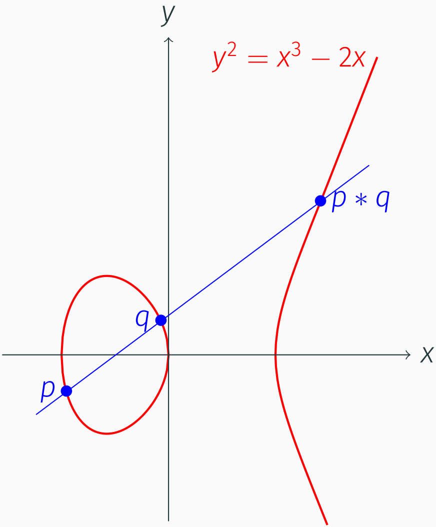
A cubic equation



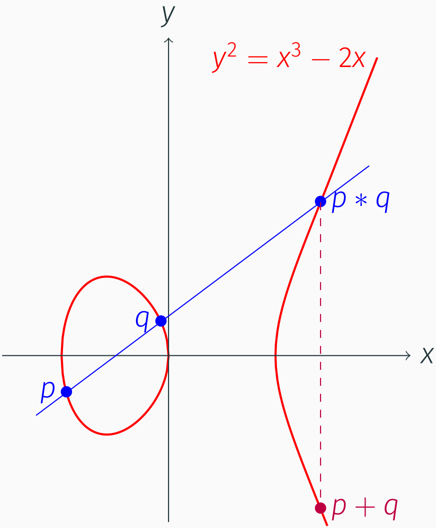
A cubic equation



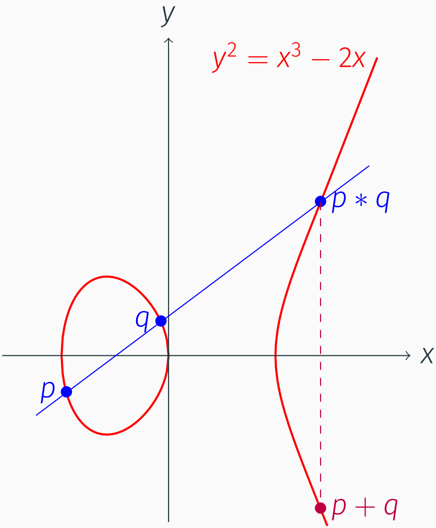
A cubic equation



A cubic equation



A cubic equation



This defines a *commutative group law* on the set of rational solutions.
The neutral element is the “point at infinity”;

Ellipti curves

Elliptic curves are those curves defined by a cubic equation of the form

$$f(x,y) = y^2 - x^3 - ax - b = 0, \qquad \Delta = -4a^3 - 27b^2 \neq 0.$$

Ellipti curves

Elliptic curves are those curves defined by a cubic equation of the form

$$f(x,y) = y^2 - x^3 - ax - b = 0, \qquad \Delta = -4a^3 - 27b^2 \neq 0.$$

The condition on the discriminant Δ states that the curve in *non singular*: if (x,y) is a singular point,

$$\frac{\partial}{\partial x} f(x,y) = \frac{\partial}{\partial y} f(x,y) = 0$$

implies that $y = 0$ and x is a multiple root of $x^3 + ax + b$.

Ellipti curves

Elliptic curves are those curves defined by a cubic equation of the form

$$f(x,y) = y^2 - x^3 - ax - b = 0, \qquad \Delta = -4a^3 - 27b^2 \neq 0.$$

The condition on the discriminant Δ states that the curve in *non singular*: if (x, y) is a singular point,

$$\frac{\partial}{\partial x} f(x,y) = \frac{\partial}{\partial y} f(x,y) = 0$$

implies that $y = 0$ and x is a multiple root of $x^3 + ax + b$.

Contrary to conics, elliptic curves cannot be parameterized by rational functions.

Elliptic curves — Another Poincaré conjecture

Let an elliptic be given by a cubic equation of the form

$$y^2 = x^3 + ax + b, \qquad \Delta = -4a^3 - 27b^2 \neq 0$$

where a and b are rational numbers.

Theorem (Mordell, 1922)

The group of rational solutions is a finitely generated abelian group.

Elliptic curves — Another Poincaré conjecture

Let an elliptic be given by a cubic equation of the form

$$y^2 = x^3 + ax + b, \qquad \Delta = -4a^3 - 27b^2 \neq 0$$

where a and b are rational numbers.

Theorem (Mordell, 1922)

The group of rational solutions is a finitely generated abelian group.

Theorem (Siegel, 1929)

There are only finitely many integer solutions.

Equations of higher degree

Let us now consider an equation of degree $\geqslant 1$, defining a *nonsingular* curve. It is important to work in the context of *projective geometry* and to forbid singularities at infinity, or complex.

Theorem (Faltings, 1983; conjectured by Mordell)

There are only finitely many rational solutions.

Equations of higher degree

Let us now consider an equation of degree $\geqslant 1$, defining a *nonsingular* curve. It is important to work in the context of *projective geometry* and to forbid singularities at infinity, or complex.

Theorem (Faltings, 1983; conjectured by Mordell)

There are only finitely many rational solutions.

Consequence : for every integer $n \geqslant 4$, the Fermat equation has only finitely many solutions.

Geometric trichotomy

Up to now, we saw three classes of equations:

- degree 1 or 2 (conics): rational parameterizations, sometimes infinitely many integer solutions;
- degree 3 (elliptic curves) : no rational parameterization, sometimes infinitely many rational solutions, finitely many integer solutions;
- degree 4 or higher : finitely many rationnal solutions.

Geometric trichotomy

Up to now, we saw three classes of equations:

- degree 1 or 2 (conics): rational parameterizations, sometimes infinitely many integer solutions;
- degree 3 (elliptic curves) : no rational parameterization, sometimes infinitely many rational solutions, finitely many integer solutions;
- degree 4 or higher : finitely many rationnal solutions.

The correct way of understanding this trichotomy requires to consider the complex solutions — they form a Riemann surface and the distinction is then

- genus 0 (Riemann sphere, positive curvature;
- genus 1 (zero curvature);
- genus 2 or higher (negative curvature).

What in higher dimension

For systems of equations whose geometry gives rise to higher dimensional varieties, the situation is wide open.

What in higher dimension

For systems of equations whose geometry gives rise to higher dimensional varieties, the situation is wide open.

Let us assume that our system of polynomial equations gives rise to a smooth complex projective variety.

The analogue of the condition “genus $\geqslant 2$” is that of a variety of general type.

What in higher dimension

For systems of equations whose geometry gives rise to higher dimensional varieties, the situation is wide open.

Let us assume that our system of polynomial equations gives rise to a smooth complex projective variety.

The analogue of the condition “genus $\geqslant 2$” is that of a variety of general type.

A conjecture of Lang then predicts that the rational solutions are contained in a strict algebraic subvariety. In other words, they satisfy an additional algebraic condition!

What in higher dimension

For systems of equations whose geometry gives rise to higher dimensional varieties, the situation is wide open.

Let us assume that our system of polynomial equations gives rise to a smooth complex projective variety.

The analogue of the condition “genus $\geqslant 2$” is that of a variety of general type.

A conjecture of Lang then predicts that the rational solutions are contained in a strict algebraic subvariety. In other words, they satisfy an additional algebraic condition!

Only (?) known cases: subvarieties of abelian varieties (Faltings, 1991).

Deciding the solvability of a diophantine equation

Hilbert's 10th problem

David Hilbert, 1900, International congress of mathematicians

Hilbert’s 10th problem

David Hilbert, 1900, International congress of mathematicians

> *Entscheidung der Lösbarkeit einer diophantischen Gleichung.*
>
> Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlkoefficienten sei vorgelegt: man soll ein Verfahren angeben, nach welchen sich mittels einer endlichen Anzahl von Operationen entscheiden lässt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.

Hilbert’s 10th problem

David Hilbert, 1900, International congress of mathematicians

Entscheidung der Lösbarkeit einer diophantischen Gleichung.

Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlkoefficienten sei vorgelegt: man soll ein Verfahren angeben, nach welchen sich mittels einer endlichen Anzahl von Operationen entscheiden lässt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.

On the possibility of solving a diophantine equation.

Let be given a diophantine equation in any number of unknownw and with coefficients in rational integers: one asks to find a method by which, using finitely many operations, one will distinguish whether the equation is solvable in rational integers.

The Entscheidungsproblem (Hilbert, 1928)

In 1928, Hilbert generalizes his 10th problem and states the decision problem (Entscheidungsproblem): the question is to prove (or disprove) the existence of an algorithme that correctly answers by yes or no every mathematical question (suitably formalized, in first order logic).

The Entscheidungsproblem (Hilbert, 1928)

In 1928, Hilbert generalizes his 10th problem and states the decision problem (Entscheidungsproblem): the question is to prove (or disprove) the existence of an algorithme that correctly answers by yes or no every mathematical question (suitably formalized, in first order logic).

1936: Gödel, Turing, Church prove that no such algorithm exists.

But what about diophantine equations?

Once the general decision problem has no positive solution, one may still hope that Hilbert's initial 10th problem has a positive solution.

But what about diophantine equations?

Once the general decision problem has no positive solution, one may still hope that Hilbert's initial 10th problem has a positive solution.

Theorem (Matyasevich, 1970)

There is no algorithm that, given an arbitrary diophantine equation, says whether or not it has a solution or rational integers.

But what about diophantine equations?

Once the general decision problem has no positive solution, one may still hope that Hilbert's initial 10th problem has a positive solution.

Theorem (Matyasevich, 1970)

There is no algorithm that, given an arbitrary diophantine equation, says whether or not it has a solution or rational integers.

Strong version: There exists a polynomial

$$f(t, x_1, \ldots, x_9) \in \mathbf{Z}[t, x_1, \ldots, x_9]$$

in 10 variables for which no algorithm can tell, given an integer $a \in \mathbf{Z}$, whether or not the equation $f(a, x_1, \ldots, x_9) = 0$ has a solution in $\mathbf{Z}^9$.

But what about diophantine equations?

Once the general decision problem has no positive solution, one may still hope that Hilbert's initial 10th problem has a positive solution.

Theorem (Matyasevich, 1970)

There is no algorithm that, given an arbitrary diophantine equation, says whether or not it has a solution or rational integers.

Strong version: There exists a polynomial

$$f(t, x_1, \ldots, x_9) \in \mathbf{Z}[t, x_1, \ldots, x_9]$$

in 10 variables for which no algorithm can tell, given an integer $a \in \mathbf{Z}$, whether or not the equation $f(a, x_1, \ldots, x_9) = 0$ has a solution in $\mathbf{Z}^9$.

For rational solutions: the question is still open!

But what about equations in 2 variables?

Let's go back to equations in 2 variables defining a nonsingular projective plane curve.

But what about equations in 2 variables?

Let's go back to equations in 2 variables defining a nonsingular projective plane curve.

In genus 0, the Hasse–Minkowski theorem allows to decide effectively whether or not the equation has a rational solution. The point is that there are only finitely many congruences to check.

But what about equations in 2 variables?

Let's go back to equations in 2 variables defining a nonsingular projective plane curve.

In genus 0, the Hasse–Minkowski theorem allows to decide effectively whether or not the equation has a rational solution. The point is that there are only finitely many congruences to check.

In genus 1, there exists an upper bound for the *size* of an integer solution (A. Baker, $\leqslant 1970$). For rational solutions, there is a device that, in practice, will sooner or later furnish generators of the group of solutions (Tate, 1974), but it is still a conjecture, because it depends on the (yet unproven) finiteness of the "Tate–Shafarevich group".

But what about equations in 2 variables?

Let's go back to equations in 2 variables defining a nonsingular projective plane curve.

In genus 0, the Hasse–Minkowski theorem allows to decide effectively whether or not the equation has a rational solution. The point is that there are only finitely many congruences to check.

In genus 1, there exists an upper bound for the *size* of an integer solution (A. Baker, $\leqslant 1970$). For rational solutions, there is a device that, in practice, will sooner or later furnish generators of the group of solutions (Tate, 1974), but it is still a conjecture, because it depends on the (yet unproven) finiteness of the "Tate–Shafarevich group".

In genus $\geqslant 2$, finding an effective version of Mordell conjecture is a completely open question.

The ABC conjecture

Conjecture (Masser, Oesterlé, 1985)

For every $\theta > 1$, there exists $K_\theta > 0$ so that the following holds:

If A, B, C are three coprime integers such that $A + B = C$, then

$$\sup(|A|, |B|, |C|) \leqslant K_\theta \big(\operatorname{rad}(ABC)\big)^\theta.$$

The *radical* $\operatorname{rad}(ABC)$ is the product of the prime numbers that divide it.

In other words, this conjecture predicts that the multiplicities of the prime factors of A, B, C are not too large.

The ABC conjecture

Conjecture (Masser, Oesterlé, 1985)

For every $\theta > 1$, there exists $K_\theta > 0$ so that the following holds:

If A, B, C are three coprime integers such that $A + B = C$, then

$$\sup(|A|, |B|, |C|) \leqslant K_\theta \big(\operatorname{rad}(ABC) \big)^\theta .$$

The *radical* $\operatorname{rad}(ABC)$ is the product of the prime numbers that divide it.

In other words, this conjecture predicts that the multiplicities of the prime factors of A, B, C are not too large.

Record (Reyssat, 1987) :

$$2 + 3^{10} \times 109 = 23^5$$

$$\theta(a, b, c) := \frac{\log(\sup(a, b, c))}{\log(\operatorname{rad}(abc))} \approx 1.63$$

Fermat's Last Theorem as a consequence the *ABC* conjecture

Let (x, y, z) be a nontrivial solution ($xyz \neq 0$) of the Fermat equation

$$x^n + y^n = z^n.$$

One may assume that x, y, z are coprime.

Set $A = x^n$, $B = y^n$, $C = z^n$.

Fermat's Last Theorem as a consequence the *ABC* conjecture

Let (x, y, z) be a nontrivial solution ($xyz \neq 0$) of the Fermat equation

$$x^n + y^n = z^n.$$

One may assume that x, y, z are coprime.

Set $A = x^n$, $B = y^n$, $C = z^n$.

Since $\operatorname{rad}(x^n y^n z^n) = \operatorname{rad}(xyz)$, assuming the truth of the *ABC* conjecture, one has

$$\sup(|x|, |y|, |z|)^n \leqslant K_\theta \big(\operatorname{rad}(xyz)\big)^\theta.$$

On the other hand, it is obvious that $\operatorname{rad}(xyz) \leqslant |x|\ |y|\ |z| \leqslant \sup(|x|, |y|, |z|)^3.$ Consequently,

$$\sup(|x|, |y|, |z|)^n \leqslant K_\theta \sup(|x|, |y|, |z|)^{3\theta},$$

hence, if $n > 3\theta$,

$$\sup(|x|, |y|, |z|) \leqslant K_\theta^{1/(n-3\theta)}.$$

Fermat's Last Theorem as a consequence the *ABC* conjecture

Let (x, y, z) be a nontrivial solution ($xyz \neq 0$) of the Fermat equation

$$x^n + y^n = z^n.$$

One may assume that x, y, z are coprime.

Set $A = x^n$, $B = y^n$, $C = z^n$.

Since $\operatorname{rad}(x^n y^n z^n) = \operatorname{rad}(xyz)$, assuming the truth of the *ABC* conjecture, one has

$$\sup(|x|, |y|, |z|)^n \leqslant K_\theta \big(\operatorname{rad}(xyz)\big)^\theta.$$

On the other hand, it is obvious that $\operatorname{rad}(xyz) \leqslant |x|\ |y|\ |z| \leqslant \sup(|x|, |y|, |z|)^3$. Consequently,

$$\sup(|x|, |y|, |z|)^n \leqslant K_\theta \sup(|x|, |y|, |z|)^{3\theta},$$

hence, if $n > 3\theta$,

$$\sup(|x|, |y|, |z|) \leqslant K_\theta^{1/(n-3\theta)}.$$

The ABC conjecture for polynomials

Theorem (Stothers, 1981; Mason, 1984)

Let $A, B, C \in \mathbf{C}[t]$ be three coprime polynomials such that $A + B = C$. Then

$$\sup(\deg(A), \deg(B), \deg(C)) \leqslant \nu(ABC) - 1$$

Here, $\nu(ABC)$ is the number of complex roots (without multiplicities) of the polynomial ABC.

The ABC conjecture for polynomials

Theorem (Stothers, 1981; Mason, 1984)

Let $A, B, C \in \mathbf{C}[t]$ be three coprime polynomials such that $A + B = C$. Then

$$\sup(\deg(A), \deg(B), \deg(C)) \leqslant \nu(ABC) - 1$$

Here, $\nu(ABC)$ is the number of complex roots (without multiplicities) of the polynomial ABC.

Proof: Set $D = AB' - A'B = AC' - A'C = CB' - C'B$.

The *ABC* conjecture for polynomials

Theorem (Stothers, 1981; Mason, 1984)

Let $A, B, C \in \mathbf{C}[t]$ *be three coprime polynomials such that* $A + B = C$*. Then*

$$\sup(\deg(A), \deg(B), \deg(C)) \leqslant \nu(ABC) - 1$$

Here, $\nu(ABC)$ is the number of complex roots (without multiplicities) of the polynomial ABC.

Proof: Set $D = AB' - A'B = AC' - A'C = CB' - C'B$.

One has $D \neq 0$, and $\deg(D) \leqslant \deg(A) + \deg(B) - 1$.

The ABC conjecture for polynomials

Theorem (Stothers, 1981; Mason, 1984)

Let $A, B, C \in \mathbf{C}[t]$ be three coprime polynomials such that $A + B = C$. Then

$$\sup(\deg(A), \deg(B), \deg(C)) \leqslant \nu(ABC) - 1$$

Here, $\nu(ABC)$ is the number of complex roots (without multiplicities) of the polynomial ABC.

Proof: Set $D = AB' - A'B = AC' - A'C = CB' - C'B$.

One has $D \neq 0$, and $\deg(D) \leqslant \deg(A) + \deg(B) - 1$.

If x is a root of A, B, or C, with multiplicity m,
it is a root of multiplicity $\geqslant m - 1$ of D, hence

$$\deg(D) \geqslant \deg(A) + \deg(B) + \deg(C) - \nu(ABC).$$

The *ABC* conjecture for polynomials

Theorem (Stothers, 1981; Mason, 1984)

Let $A, B, C \in \mathbf{C}[t]$ *be three coprime polynomials such that* $A + B = C$*. Then*

$$\sup(\deg(A), \deg(B), \deg(C)) \leqslant \nu(ABC) - 1$$

Here, $\nu(ABC)$ is the number of complex roots (without multiplicities) of the polynomial ABC.

Proof: Set $D = AB' - A'B = AC' - A'C = CB' - C'B$.

One has $D \neq 0$, and $\deg(D) \leqslant \deg(A) + \deg(B) - 1$.

If x is a root of A, B, or C, with multiplicity m,
it is a root of multiplicity $\geqslant m - 1$ of D, hence

$$\deg(D) \geqslant \deg(A) + \deg(B) + \deg(C) - \nu(ABC).$$

Then $\deg(C) \leqslant \nu(ABC) - 1$ and similarly for $\deg(A)$ and $\deg(B)$.

Application to geometric irrationality

Thanks to the Sothers–Mason theorem, the same argument than for ABC $\Rightarrow$ Fermat *proves* that for $n \geqslant 3$, the Fermat curve cannot be parameterized by rational functions.

Application to geometric irrationality

Thanks to the Sothers–Mason theorem, the same argument than for ABC $\Rightarrow$ Fermat *proves* that for $n \geqslant 3$, the Fermat curve cannot be parameterized by rational functions.

Let $P^n + Q^n = R^n$, for three coprime polynomials $P, Q, R \in \mathbf{C}[t]$. Then

$$\begin{aligned} n \sup(\deg(P), \deg(Q), \deg(R)) &\leqslant \nu(PQR) - 1 \\ &\leqslant \deg(P) + \deg(Q) + \deg(R) - 1 \\ &< 3 \sup(\deg(P), \deg(Q), \deg(R)), \end{aligned}$$

hence $n < 3$.

ABC $\Rightarrow$ Mordell

Theorem (Elkies, 1991)

If the ABC conjecture is true, the "effective" version of Mordell conjecture is true as well: one can give an explicit bound for the size of the solutions.

Principle: Construct a rational function ϕ of x and y whose restriction to the plane curve is unramified everywhere but possibly above $0, 1, \infty$.

ABC $\Rightarrow$ Mordell

Theorem (Elkies, 1991)

If the ABC conjecture is true, the "effective" version of Mordell conjecture is true as well: one can give an explicit bound for the size of the solutions.

Principle: Construct a rational function ϕ of x and y whose restriction to the plane curve is unramified everywhere but possibly above $0, 1, \infty$.

Apply the *ABC* conjecture to the relation $\phi(P) + (1 - \phi(P)) = 1$, and conclude.

Theorem (Elkies, 1991)

If the ABC conjecture is true, the "effective" version of Mordell conjecture is true as well: one can give an explicit bound for the size of the solutions.

Principle: Construct a rational function ϕ of x and y whose restriction to the plane curve is unramified everywhere but possibly above $0, 1, \infty$.

Apply the *ABC* conjecture to the relation $\phi(P) + (1 - \phi(P)) = 1$, and conclude.

Conversely:

Theorem (Moret-Bailly, Szpiro, 1990)

An effective version of Mordell conjecture would imply the ABC conjecture (with some exponent rather than $1 + \varepsilon$).

Proving the *ABC* conjecture?

September, 17, 2012, New York Times :

A Possible Breakthrough in Explaining a Mathematical Riddle

September, 17, 2012, New York Times :
A Possible Breakthrough in Explaining a Mathematical Riddle

9 mai 2013, `http://projectwordsworth.com/the-paradox-of-the-proof/` :
The Paradox of the Proof

« I decided, I can' t possibly work on this. It would drive me nuts. »

« You don' t get to say you' ve proved something if you haven' t explained it. A proof is a social construct. If the community doesn' t understand it, you haven' t done your job. »

Proving the *ABC* conjecture?

September, 17, 2012, New York Times :
A Possible Breakthrough in Explaining a Mathematical Riddle

9 mai 2013, `http://projectwordsworth.com/the-paradox-of-the-proof/` :
The Paradox of the Proof

« I decided, I can't possibly work on this. It would drive me nuts. »

« You don't get to say you've proved something if you haven't explained it. A proof is a social construct. If the community doesn't understand it, you haven't done your job. »

August 2018, Peter Scholze, Jakob Stix :
Why abc *is still a conjecture*