1, 2, 3··· *A*, *B*, *C*···

Antoine Chambert-Loir

10 août 2021

Université de Paris

Festival d'astronomie de Fleurance

Équations diophantiennes

Encyclopédie de Diderot et d'Alembert (1751–1772)

DIOPHANTE, (*Problèmes ou questions de*) On appelle ainsi certaines questions sur les nombres quarrés, cubes, les triangles rectangles, *&c.* du genre de celles qui ont été examinées & résolues autrefois par *Diophante*, mathématicien d'Alexandrie, qu'on croit avoir vêcu vers le troisieme siecle. Nous avons son ouvrage qui a été commenté & publié à Paris en 1621, par Bachet de Meziriac; il y a une autre édition faite en 1670, avec des observations de M. Fermat sur quelques-unes des questions de *Diophante*. Dans ces questions il s'agit de trouver des nombres commensurables qui satisfassent à des problèmes in-

Encyclopédie de Diderot et d'Alembert

déterminés, auxquels satisferoient une infinité de nombres incommensurables. Par exemple, on propose de trouver un triangle rectangle dont les côtés x, y, z, soient exprimés par des nombres commensurables. Il est certain qu'on aura en général $xx + yy = zz$, z étant supposée l'hypothenuse. *Voy.* HYPOTHENUSE. Mais on voit aussi que l'on peut prendre x & y, tels que z soit un incommensurable; car si, par exemple, $x = 1$ & $y = 2$, on aura $z = \sqrt{5}$. Or il s'agit de déterminer x & y à être tels, que non seulement x & y, mais encore z soient des nombres commensurables. De même soit proposé de partager un nombre quarré a^2 en deux autres nombres qui soient aussi quarrés, & ainsi des autres. Voilà ce qu'on appelle les *questions de Diophante.*

L'art de résoudre ces sortes de questions consiste à employer & à manier tellement les inconnues ou l'inconnue, que le quarré & les plus hautes puissances de cette inconnue disparoissent de l'équation, & qu'il ne reste que l'inconnue élevée au premier degré, au moyen de quoi on résout cette équation sans avoir recours aux incommensurables. Donnons-en un exemple sur les triangles rectangles en nombres. On propose de trouver x, y, z, telles que $xx + yy = zz$: soit supposé $z = x + u$, on aura $xx + yy = xx + 2xu + uu$; d'où l'on voit qu'on peut faire disparoître xx, & qu'on aura $\frac{yy - uu}{2u} = x$; donc prenant y & u pour tout ce qu'on voudra, on trouvera que les côtés du triangle sont y, $\frac{yy - uu}{2u}$, & l'hypothenuse $x + u = \frac{yy + uu}{2u}$: par exemple, soit $y = 3$, $u = 1$, on aura $\frac{yy - uu}{2u} = \frac{8}{2} = 4$, & $x + u = \frac{10}{2} = 5$. Ainsi 3, 4, sont les deux côtés du triangle, & 5 l'hypothenuse. On voit aisément que ce problème a une infinité de solutions.

Autre problème. Soit proposé de trouver une quantité x, telle que $a + bx + xx$ soit un quarré, on fera de même $a + bx + xx$ égale au quarré de $x + z$, & on aura $a + bx = 2xz + zz$; donc $x = \frac{a - zz}{2z - b}$. Ainsi prenant z pour tout ce qu'on voudra, on aura x.

Autre. Soit proposé de partager un nombre $a^2 + b^2$, composé de deux quarrés en deux autres quarrés; soit $sx - a$, l'un des nombres cherchés, & $rx - b$ l'autre, s & r étant des coefficiens indéterminés, on aura $a^2 + b^2 = s^2x^2 - 2sxa + a^2 + r^2x^2 - 2rxb + bb$; donc $s^2x - 2sa + r^2x - 2rb = 0$; donc $x = \frac{2sa + 2rb}{r^2 + s^2}$. Ainsi prenant pour r & s tel nombre qu'on voudra, on aura x.

Autre. Soit proposé de trouver x, telle que $aa - xx$ soit un quarré. Je fais $\sqrt{aa - xx} = (a - x)z$, & j'ai $aa - xx = \overline{a - x}^2 zz$, & divisant par $a - x$, j'ai $a + x = az - xzz$; donc $\frac{az - a}{z + 1} = x$. Ainsi prenant pour z tout ce qu'on voudra, on aura x.

Voilà, ce me semble, un nombre suffisant d'exemples pour donner dans un ouvrage tel que l'Encyclopédie, l'idée des problèmes de *Diophante.* Ceux qui voudront étudier plus à fond cette matiere, la trouveront très-bien traitée dans les *élémens d'Algebre de* Saunderson, *in*-4°. *Cambridge* 1740, *liv. VI. t. II.* M. Euler dans différens volumes des mémoires de Petersbourg, a donné aussi d'une maniere très-savante la solution de plusieurs problèmes du genre de ceux de *Diophante.*

Remarquons en passant que cette méthode de réduire à des quantités rationnelles les quantités irrationnelles, est fort utile dans le calcul intégral, pour réduire une différentielle donnée en fraction rationnelle. *Voyez* CALCUL INTÉGRAL, FRACTION RATIONNELLE.

En effet soit donné $\frac{dx}{\sqrt{a + bx + xx}}$, on transformera

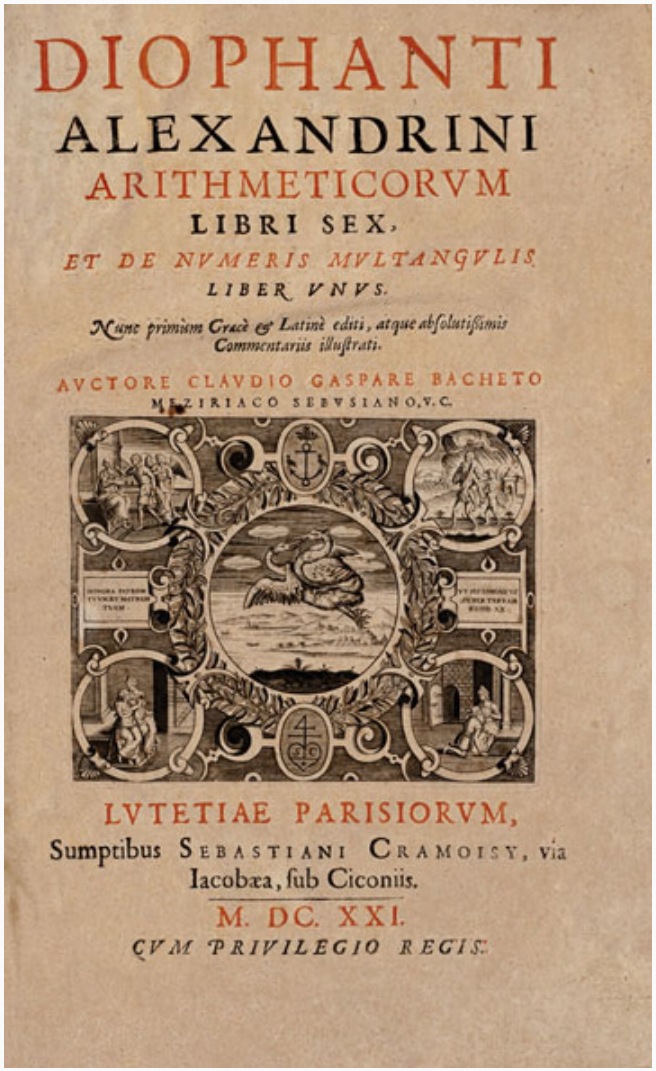
cette quantité en fraction rationnelle en supposant comme ci-dessus $x + z = \sqrt{a + bx + xx}$: on transformeroit de même $\frac{dx}{\sqrt{a + bx - xx}}$, en supposant que $p - x$ est un facteur de $a + bx - xx$, & faisant $\sqrt{a + bx - xx} = (p - x)z$. *Voyez le mémoire* que j'ai donné sur ce sujet dans le volume de l'académie de Berlin, pour l'année 1746. *Voyez* aussi le *traité du calcul intégral de* M. de Bougainville le jeune, *I. part.* chap. *des transformations des différentielles.*

« L'ouvrage de *Diophante* est, dit M. Saunderson, » le premier ouvrage d'Algebre que nous trouvions » dans l'antiquité. Ce n'est pas qu'il soit l'inventeur » de cet art; car outre qu'on trouve quelques traces » dans des auteurs plus anciens, *Diophante* ne donne point dans son ouvrage les regles de l'Algebre: » il traite cette science comme déjà connue ».

M. Saunderson fait ensuite un grand éloge de la sagacité que *Diophante* a montrée dans la solution des problèmes qui ont retenu son nom. Il ajoûte que du tems de *Diophante*, on ne connoissoit point encore la méthode de nommer par des lettres les nombres connus, comme on fait les nombres inconnus, ni la méthode d'introduire plusieurs lettres pour désigner plusieurs quantités inconnues différentes; il reconnoît que faute de cet avantage, on trouve quelquefois dans les solutions de *Diophante* un peu de confusion. Nous n'examinerons point ici si ce qu'on trouve dans l'ouvrage de *Diophante* peut être regardé comme de l'Algebre; & supposé que c'en soit en effet, jusqu'où les anciens paroissent avoir poussé cette science. C'est une question qui nous conduiroit trop loin, qui n'appartient qu'indirectement à cet article, & que nous pourrons avoir occasion de traiter ailleurs. *Voyez* ALGEBRE & MATHÉMATIQUES. (*O*)

DIOPTRE, s. m. (*Chirurgie.*) instrument qui sert à dilater la matrice ou l'anus, afin d'examiner les maladies de ces parties. On l'appelle aussi *Speculum*

Diophante — Arithmétique

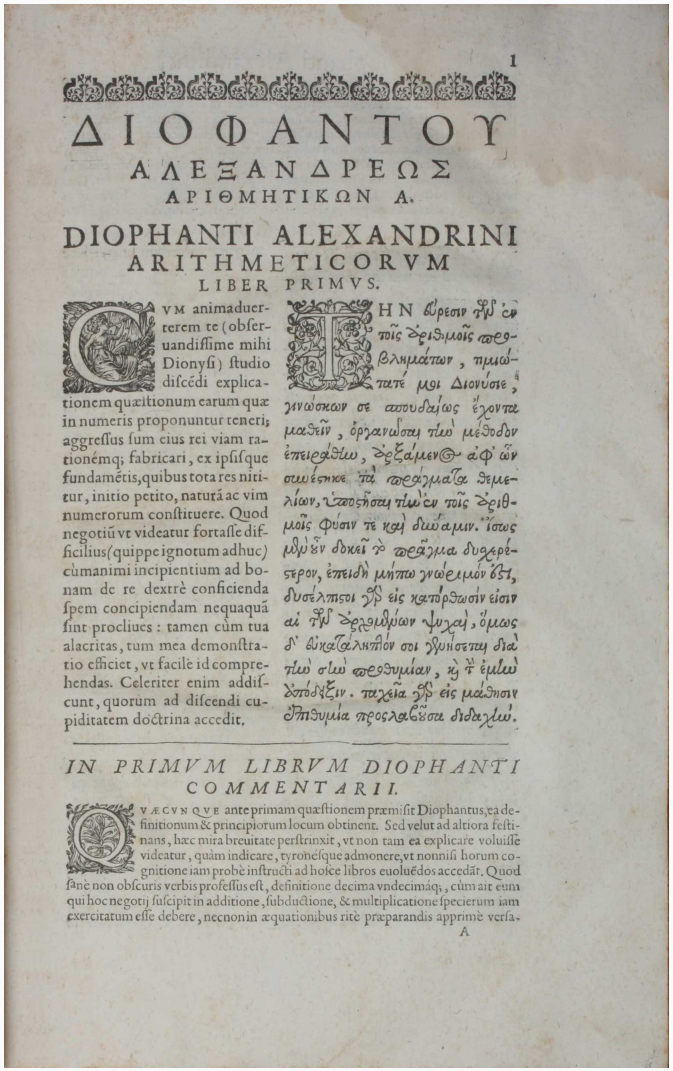


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.

Nunc primùm Græcè & Latinè editi, atque absolutissimis Commentariis illustrati.

AVCTORE CLAVDIO GASPARE BACHETO
MEZIRIACO SEBVSIANO, V.C.

LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS.



1

ΔΙΟΦΑΝΤΟΥ
ΑΛΕΞΑΝΔΡΕΩΣ
ΑΡΙΘΜΗΤΙΚΩΝ Α.

DIOPHANTI ALEXANDRINI
ARITHMETICORVM
LIBER PRIMVS.

CVM animaduerterem te (obseruandissime mihi Dionysi) studio discēdi explicationem quæstionum earum quæ in numeris proponuntur teneri; aggressus sum eius rei viam rationémq; fabricari, ex ipsisque fundamētis, quibus tota res nititur, initio petito, naturā ac vim numerorum constituere. Quod negotiū vt videatur fortasse difficilius (quippe ignotum adhuc) cùmanimi incipientium ad bonam de re dextrè conficienda spem concipiendam nequaquā sint proclives: tamen cùm tua alacritas, tum mea demonstratio efficiet, vt facilè id comprehendas. Celeriter enim addiscunt, quorum ad discendi cupiditatem doctrina accedit.

ΗΝ ἕυρεσιν τῶν ἐν τοῖς ἀριθμοῖς προβλημάτων, πυμώτατέ μοι Διονύσιε, γινώσκων σε ασπουδαίως ἔχοντα μαθεῖν, ὀργανῶσαι πῶς μέθοδον ἐπειρᾶτο, ἀρξάμενος ἀφ' ὧν συνέστηκε τὰ πρόβλματα θεμελίων, ὑποστῆσαι πῶς ἐν τοῖς ἀριθμοῖς φύσιν τε καὶ δύναμιν. ἴσως μὲν οὖν δοκεῖ τὸ πρᾶγμα δυσχερέστερον, ἐπειδὴ μήπω γνώριμόν ἐστι, δυσέλπιστοι γὰρ εἰς κατόρθωσιν εἰσὶν αἱ τῶν ἀρχομένων ψυχαί, ὅμως δ' δικαιοτέλεσπόν σοι γενήσεται διὰ πολὺ σὸν προθυμίαν, καὶ τὴν ἐμὴν ἀποδείξιν. ταχεῖα γὰρ εἰς μάθησιν ἐπιθυμία προσλαβοῦσα διδαχήν.

IN PRIMVM LIBRVM DIOPHANTI COMMENTARII.

VÆCVNQVE ante primam quæstionem præmisit Diophantus, ea definitionum & principiorum locum obtinent. Sed velut ad altiora festinans, hæc mira breuitate perstrinxit, vt non tam ea explicare voluisse videatur, quàm indicare, tyronesque admonere, vt nonnisi horum cognitione iam probè instructi ad hoce libros euoluēdos accedāt. Quod sanè non obscuris verbis professus est, definitione decima vndecimáq;, cùm ait eum qui hoc negotij suscipit in additione, subductione, & multiplicatione specierum iam exercitatum esse debere, necnon in æquationibus ritè præparandis apprimè versa-

A

Équations diophantiennes

Équations *diophantiennes* :

- les inconnues sont des nombres entiers ou rationnels ;
- les équations sont données par des relations polynomiales entre les inconnues

Équations diophantiennes

Équations *diophantiennes* :

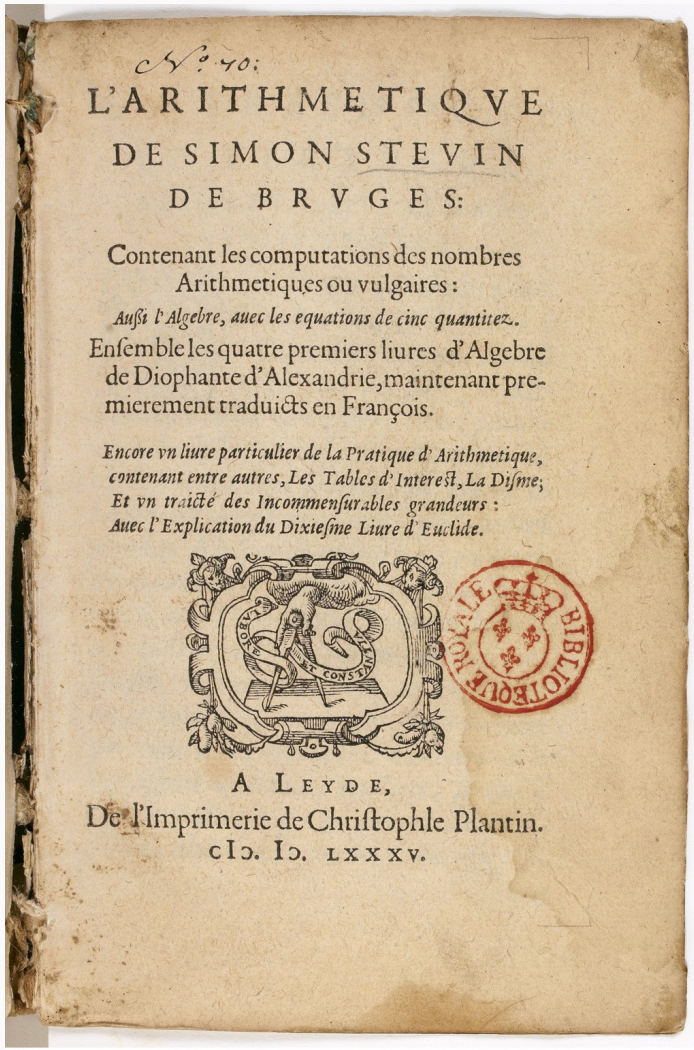
- les inconnues sont des nombres entiers ou rationnels ;
- les équations sont données par des relations polynomiales entre les inconnues

Grossièrement, trois paramètres :

- le nombre de variables ;
- le nombre d'équations ;
- le degré des équations, c'est-à-dire le plus grand nombre de fois que des inconnues sont multipliées entre elles dans une équation.

L'*Arithmétique* expose toute une série de problèmes de ce genre, avec leurs solutions.

Simon Stévin



N°. 40.

L'ARITHMETIQVE
DE SIMON STEVIN
DE BRVGES:

Contenant les computations des nombres Arithmetiques ou vulgaires :

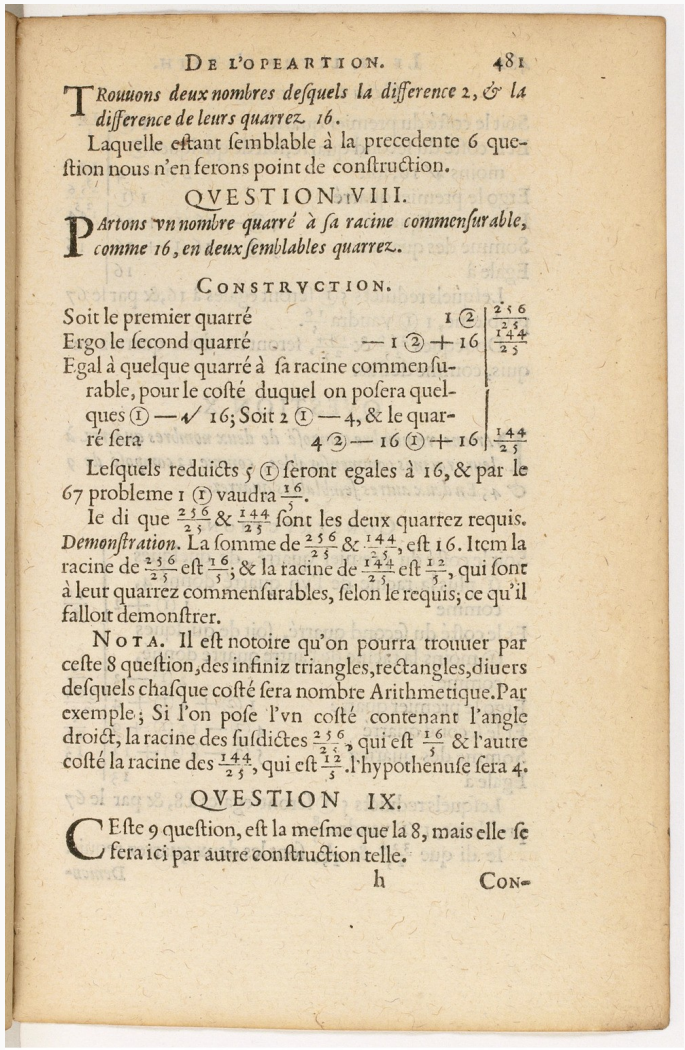
Aussi l'Algebre, auec les equations de cinc quantitez.

Ensemble les quatre premiers liures d'Algebre de Diophante d'Alexandrie, maintenant premierement traduicts en François.

Encore vn liure particulier de la Pratique d'Arithmetique, contenant entre autres, Les Tables d'Interest, La Disme; Et vn traicté des Incommensurables grandeurs : Auec l'Explication du Dixiesme Liure d'Euclide.

A LEYDE,
De l'Imprimerie de Christophle Plantin.
cIↃ. IↃ. LXXXV.

Source gallica.bnf.fr / Bibliothèque nationale de France



DE L'OPEARTION. 481

Trouuons deux nombres desquels la difference 2, & la difference de leurs quarrez 16.

Laquelle estant semblable à la precedente 6 question nous n'en ferons point de construction.

QVESTION VIII.

Partons vn nombre quarré à sa racine commensurable, comme 16, en deux semblables quarrez.

CONSTRVCTION.

Soit le premier quarré $1 ② \quad \frac{256}{25}$
Ergo le second quarré $— 1 ② + 16 \quad \frac{144}{25}$
Egal à quelque quarré à sa racine commensurable, pour le costé duquel on posera quelques ① $— \sqrt{16}$; Soit 2 ① — 4, & le quarré sera $4 ② — 16 ① + 16 \quad \frac{144}{25}$

Lesquels reduicts 5 ① seront egales à 16, & par le 67 probleme 1 ① vaudra $\frac{16}{5}$.

Ie di que $\frac{256}{25}$ & $\frac{144}{25}$ sont les deux quarrez requis. *Demonstration.* La somme de $\frac{256}{25}$ & $\frac{144}{25}$, est 16. Item la racine de $\frac{256}{25}$ est $\frac{16}{5}$; & la racine de $\frac{144}{25}$ est $\frac{12}{5}$, qui sont à leur quarrez commensurables, selon le requis; ce qu'il falloit demonstrer.

NOTA. Il est notoire qu'on pourra trouuer par ceste 8 question, des infiniz triangles, rectangles, diuers desquels chasque costé sera nombre Arithmetique. Par exemple; Si l'on pose l'vn costé contenant l'angle droict, la racine des susdictes $\frac{256}{25}$, qui est $\frac{16}{5}$ & l'autre costé la racine des $\frac{144}{25}$, qui est $\frac{12}{5}$. l'hypothenuse sera 4.

QVESTION IX.

CEste 9 question, est la mesme que la 8, mais elle se fera ici par autre construction telle.

h CON-

Source gallica.bnf.fr / Bibliothèque nationale de France

Échauffement : équations en une variable

Les équations diophantiennes en une variable sont faciles à résoudre.

Échauffement : équations en une variable

Les équations diophantiennes en une variable sont faciles à résoudre.

Théorème

Soit $a_0, \ldots, a_{n-1}, a_n \in \mathbf{C}$, *avec* $a_n \neq 0$.

Toute racine x *de l'équation de degré* n *:*

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

vérifie

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

Échauffement : équations en une variable

Les équations diophantiennes en une variable sont faciles à résoudre.

Théorème

Soit $a_0, \ldots, a_{n-1}, a_n \in \mathbf{C}$, *avec* $a_n \neq 0$.

Toute racine x *de l'équation de degré* n *:*

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

vérifie

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

Il suffit donc d'essayer un à un tous les entiers dans l'intervalle décrit par l'inégalité du théorème...

Équations en une variable : divisibilité

Si l'on cherche des solutions en nombres rationnels, un critère classique permet de se ramener au cas de solutions en nombres entiers.

Théorème

Soit $a_0, \ldots, a_{n-1}, a_n \in \mathbf{Z}$, avec $a_n \neq 0$. Soit $x = p/q$ une solution rationnelle de l'équation de degré n :

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

Si p et q sont sans facteur commun, alors q divise a_n et p divise a_0.

En particulier, si $a_n = 1$, alors toutes les solutions rationnelles sont en fait entières.

La géométrie des équations diophantiennes

Équations de degré 1

Un vieux problème (III-Ve s. ap. J.-C.) :

Équations de degré 1

Un vieux problème (III-Ve s. ap. J.-C.) :

> 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？

Équations de degré 1

Un vieux problème (III-Ve s. ap. J.-C.) :

> 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？

c'est-à-dire :

> *Un nombre de choses est inconnu. Si on les compte par trois, il en reste 2; si on les compte par cinq, il en reste 3; si on les compte par sept, il en reste 2. Trouver ce nombre de choses.*

Équations de degré 1

Un vieux problème (III-Ve s. ap. J.-C.) :

> 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？

c'est-à-dire :

> *Un nombre de choses est inconnu. Si on les compte par trois, il en reste 2; si on les compte par cinq, il en reste 3; si on les compte par sept, il en reste 2. Trouver ce nombre de choses.*

Ce problème « chinois » est dû à Sūnzǐ, publié dans le Sūnzǐ Suàngjīng 孫子算經 *Le classique mathématique de Sūnzǐ*.

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釐十釐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 d'une page d'une édition de la dynastie Qing (1644 – 1912)

Source : *Wikipedia*

Le problème chinois

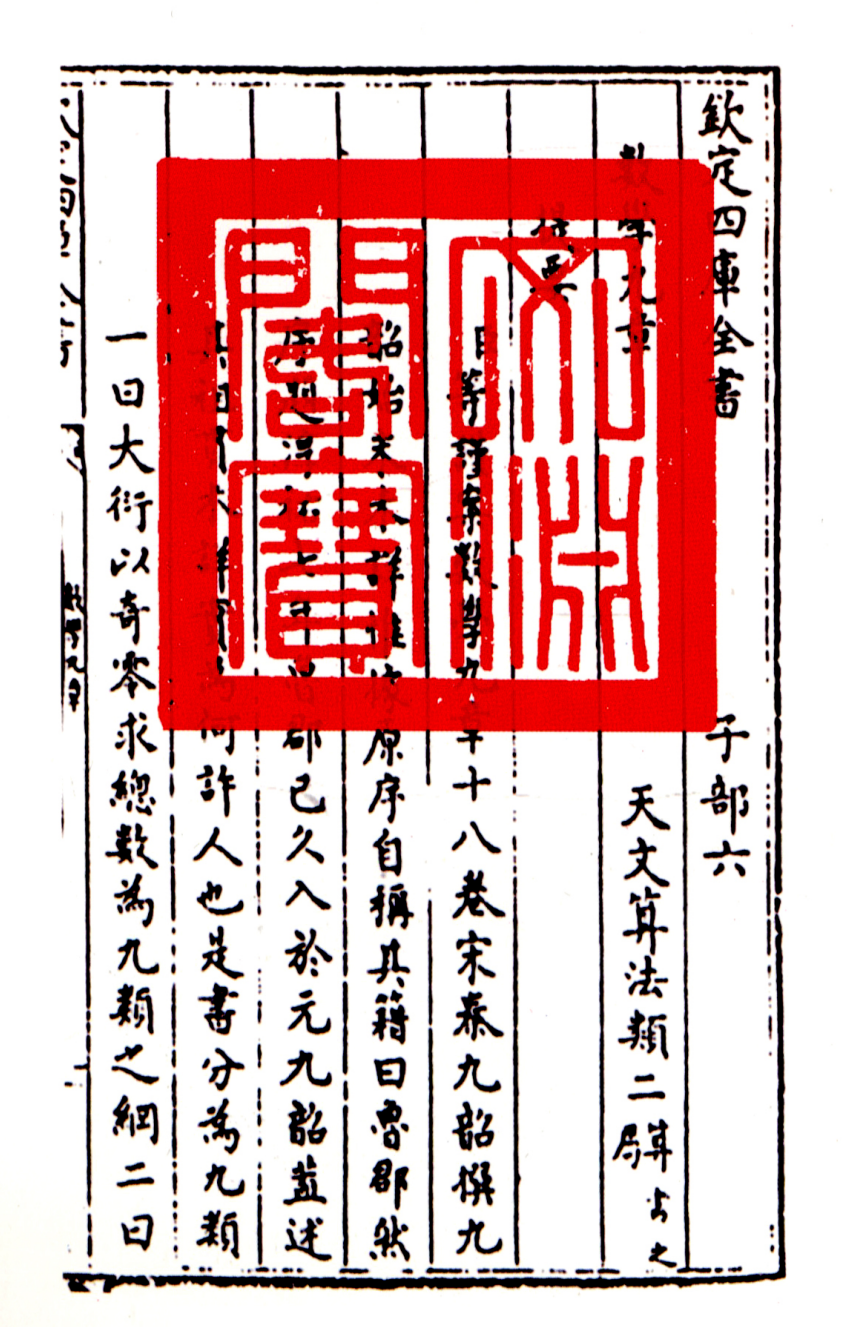
Ce genre d'exercices a ensuite été reproduit dans d'autres manuels, comme le

Shùshū Jiǔzhāng —數書九章,
Traîté mathématique en neuf sections, 1247,

lui-même inclus dans le

Sìkù quánshū —四庫全書,
Le recueil complet des quatre trésors, XIXe s.,

une sorte d'encyclopédie commandée par les empereurs Qing pour prouver qu'ils surpassaient l'Encyclopédie Ming (environ 1403).



Traîté mathématique en neuf sections
(數書九章, Shùshū Jiǔzhāng)
reproduction du Sìkù Quánshū 四庫全書 (1847)

Source : *Wikipedia*

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？

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？

c'est-à-dire :

Un nombre de choses est inconnu. Si on les compte par trois, il en reste 2; si on les compte par cinq, il en reste 3; si on les compte par sept, il en reste 2. Trouver ce nombre de choses.

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？

c'est-à-dire :

> *Un nombre de choses est inconnu. Si on les compte par trois, il en reste 2; si on les compte par cinq, il en reste 3; si on les compte par sept, il en reste 2. Trouver ce nombre de choses.*

soit encore :

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

l'inconnue principale étant n.

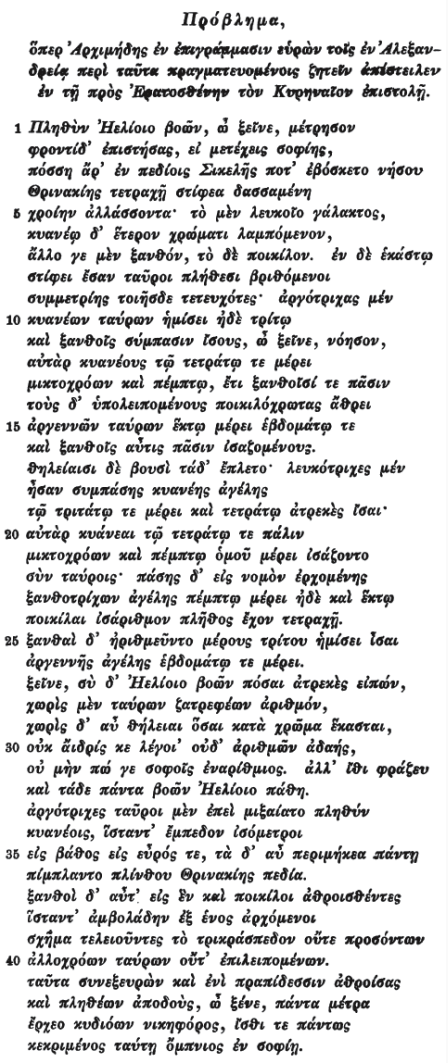
Le « théorème chinois » apprend que la plus petite solution est $n = 23$ et que toutes les autres sont obtenues en ajoutant un multiple de $105 = 3 \times 5 \times 7$.

Πρόβλημα,

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

1 Πληθὺν Ἠελίοιο βοῶν, ὦ ξεῖνε, μέτρησον
φροντίδ' ἐπιστήσας, εἰ μετέχεις σοφίης,
πόσση ἄρ' ἐν πεδίοις Σικελῆς ποτ' ἐβόσκετο νήσου
Θρινακίης τετραχῇ στίφεα δασσαμένη
5 χροίην 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
10 κυανέων ταύρων ἡμίσει ἠδὲ τρίτῳ
καὶ ξανθοῖς σύμπασιν ἴσους, ὦ ξεῖνε, νόησον,

Équations de degré 2



Πρόβλημα,

ὅπερ Ἀρχιμήδης ἐν ἐπιγράμμασιν εὑρὼν τοῖς ἐν Ἀλεξανδρείᾳ περὶ ταῦτα πραγματευομένοις ζητεῖν ἐπέστειλεν 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
χροίην 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 ἴσαι·
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 ἴσαι
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, ἵστανθ' 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.

Le problème des bœufs d'Archimède

Archimedis Opera omnia, cum commentariis Eutocii

Édité par J. L. Heiberg

B. G. Teubner, Leibzig, Volume 2 (1881), pages 448–450

Le problème des bœufs d'Archimède : première partie

Il y a a quatre troupeaux de bœufs, vaches et taureaux, de quatre couleurs : blanc (w et W), noir (b et B), jaune (y et Y) et pommelé (d et D).

Le texte donne des proportions :

$$\begin{aligned} W &= \left(\tfrac{1}{2} + \tfrac{1}{3}\right)B + Y \\ B &= \left(\tfrac{1}{4} + \tfrac{1}{5}\right)D + Y \\ D &= \left(\tfrac{1}{6} + \tfrac{1}{7}\right)W + Y \end{aligned}$$

$$\begin{aligned} w &= \left(\tfrac{1}{3} + \tfrac{1}{4}\right)(B + b) \\ b &= \left(\tfrac{1}{4} + \tfrac{1}{5}\right)(Y + y) \\ d &= \left(\tfrac{1}{5} + \tfrac{1}{6}\right)(Y + y) \\ y &= \left(\tfrac{1}{6} + \tfrac{1}{7}\right)(W + w) \end{aligned}$$

C'est un problème linéaire.

Le problème des bœufs d'Archimède : première partie

C'est un problème linéaire en nombres entiers, qui peut être résolu en nombres rationnels par la méthode habituelle de Gauss, et c'est plus facile si on dispose d'un logiciel de calcul algébrique. En chassant les dénominateurs, on trouve

$$\begin{aligned} W &= 10,366,482 \cdot n & w &= 7,206,360 \cdot n \\ B &= 7,460,514 \cdot n & b &= 4,893,246 \cdot n \\ Y &= 4,149,387 \cdot n & y &= 5,439,213 \cdot n \\ D &= 7,358,060 \cdot n & d &= 3,515,820 \cdot n \end{aligned}$$

où n est un entier (commun).

Le problème des bœufs d'Archimède : seconde partie

Mais ce n'est pas fini !

Le problème des bœufs d'Archimède : seconde partie

Mais ce n'est pas fini ! Car Archimède indique : « *on ne te dira pas maladroit, ou ignorant des nombres, mais ce n'est pas encore qu'on se souviendra de toi parmi les sages* ». Pour cela, il s'agit de résoudre la seconde partie du problème :

$$W + B \text{ est un carré parfait, de la forme } p^2$$
$$Y + D \text{ est un nombre triangulaire, de la forme } m(m+1)/2$$

Le problème des bœufs d'Archimède : seconde partie

Mais ce n'est pas fini ! Car Archimède indique : « *on ne te dira pas maladroit, ou ignorant des nombres, mais ce n'est pas encore qu'on se souviendra de toi parmi les sages* ». Pour cela, il s'agit de résoudre la seconde partie du problème :

$W + B$ est un carré parfait, de la forme p^2
$Y + D$ est un nombre triangulaire, de la forme $m(m+1)/2$

C'est-à-dire :

$$17,826,996 \cdot n = p^2$$

$$11,507,447 \cdot n = m(m+1)/2$$

Le problème des bœufs d'Archimède : seconde partie

Grâce à la factorisation

$$17,826,996 = 2^2 \cdot 3 \cdot 11 \cdot 29 \cdot 4657,$$

on obtient

$$n = 3 \cdot 11 \cdot 29 \cdot 4657 \cdot k^2 = 4,456,749k^2.$$

On récrit cette équation comme

$$11,507,447 \cdot n = m(m+1)/2,$$

une équation de degré 2 en l'inconnue m, où n est un paramètre. On veut que $1 + 92,059,576 \cdot n$ soit un carré parfait, q^2, d'où l'équation

$$q^2 - 410,286,423,278,424 \cdot k^2 = 1.$$

L'équation de Brahmagupta (Pell-Fermat)

Le problème d'Archimède mène à l'équation

$$q^2 - 410,286,423,278,424 \cdot k^2 = 1.$$

On trouve que le nombre total d'animaux est un nombre à 413 091 chiffres ! (Vardi)

Pour aujourd'hui, on pourrait se contenter de remplacer ce nombre énorme par un plus petit, non ?

L'équation de Brahmagupta (Pell-Fermat)

Le problème d'Archimède mène à l'équation

$$q^2 - 410,286,423,278,424 \cdot k^2 = 1.$$

On trouve que le nombre total d'animaux est un nombre à 413 091 chiffres ! (Vardi)

Pour aujourd'hui, on pourrait se contenter de remplacer ce nombre énorme par un plus petit, non ?

Si n est un paramètre (non carré), il s'agit de trouver les solutions en nombres entiers de l'équation

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

L'équation de Brahmagupta (Pell-Fermat)

Le problème d'Archimède mène à l'équation

$$q^2 - 410,286,423,278,424 \cdot k^2 = 1.$$

On trouve que le nombre total d'animaux est un nombre à 413 091 chiffres ! (Vardi)

Pour aujourd'hui, on pourrait se contenter de remplacer ce nombre énorme par un plus petit, non ?

Si n est un paramètre (non carré), il s'agit de trouver les solutions en nombres entiers de l'équation

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

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

Résoudre l'équation de Brahmagupta : l'identité de Brahmagupta

Brahmagupta (628 ap. J.C.) :

मूलं द्विघेष्टवर्गाद् गुणक गुणादिष्टयुत विहीनाच्च ।
आद्यवधो गुणकगुणः सहान्त्यघातेन कृतमन्त्यम् ॥
वज्रवधैक्यं प्रथमं प्रक्षेपः क्षेपवध तुल्यः ।
प्रक्षेपशोधकहृते मूले प्रक्षेपके रूपे ॥

—*BrSpSi. XVIII 64-65*

Résoudre l'équation de Brahmagupta : l'identité de Brahmagupta

Brahmagupta (628 ap. J.C.) :

मूलं द्विघेष्टवर्गाद् गुणक गुणादिष्टयुत विहीनाच्च ।
आद्यवधो गुणकगुणः सहान्त्यघातेन कृतमन्त्यम् ॥
वज्रवधैक्यं प्रथमं प्रक्षेपः क्षेपवध तुल्यः ।
प्रक्षेपशोधकहृते मूले प्रक्षेपके रूपे ॥

—*BrSpSi. XVIII 64-65*

Si (x, y) et (x', y') sont des solutions, on peut en construire une troisième (x'', y'') par la formule :

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

Résoudre l'équation de Brahmagupta : l'identité de Brahmagupta

Brahmagupta (628 ap. J.C.) :

मूलं द्विघेष्टवर्गाद् गुणक गुणादिष्टयुत विहीनाच्च ।
आद्यवधो गुणकगुणः सहान्त्यघातेन कृतमन्त्यम् ॥
वज्रवधैक्यं प्रथमं प्रक्षेपः क्षेपवध तुल्यः ।
प्रक्षेपशोधकहृते मूले प्रक्षेपके रूपे ॥

—*BrSpSi. XVIII 64-65*

Si (x, y) et (x', y') sont des solutions, on peut en construire une troisième (x'', y'') par la formule :

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

Toutes les solutions (ou presque) sont obtenues à partir d'une solution minimale.

Résoudre l'équation de Brahmagupta : l'identité de Brahmagupta

Explication moderne de l'identité de Brahamagupta :

On observe que

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

est le produit du nombre quadratique $x + \sqrt{n}y$ par son « conjugué » $x - \sqrt{n}y$ obtenu en changeant le signe de la racine carrée – analogue de la relation $x^2 + y^2 = (x + iy)(x - iy)$.

C'est une sorte que *norme carrée* d'un nombre quadratique, et elle est multiplicative comme pour les nombres complexes. On a :

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

L'équation de Pythagore

Il s'agit de trouver les solutions de l'équation

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

L'équation de Pythagore

Il s'agit de trouver les solutions de l'équation

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

Seules solutions entières : $(\pm 1, 0)$, $(0, \pm 1)$.

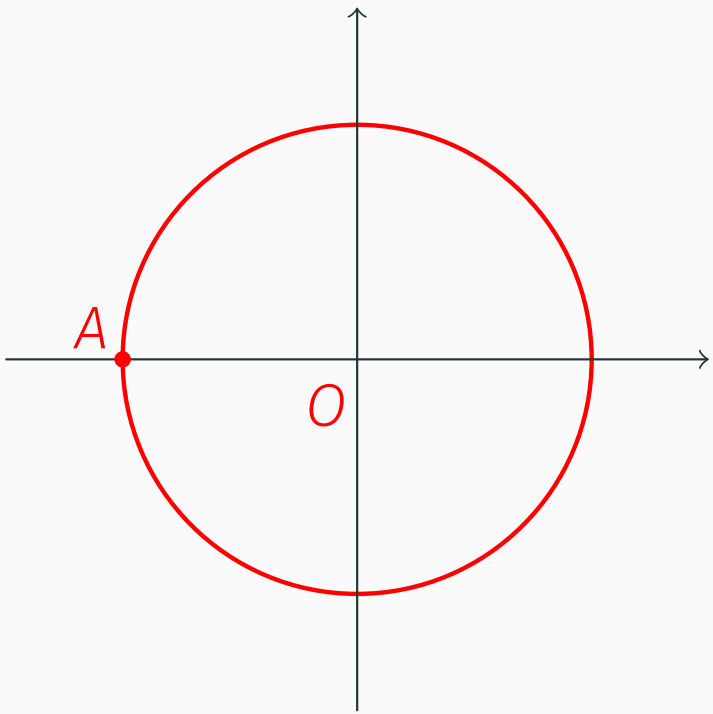
L'équation de Pythagore

Il s'agit de trouver les solutions de l'équation

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

Seules solutions entières : $(\pm 1, 0)$, $(0, \pm 1)$.

Solutions en nombres rationnels ?



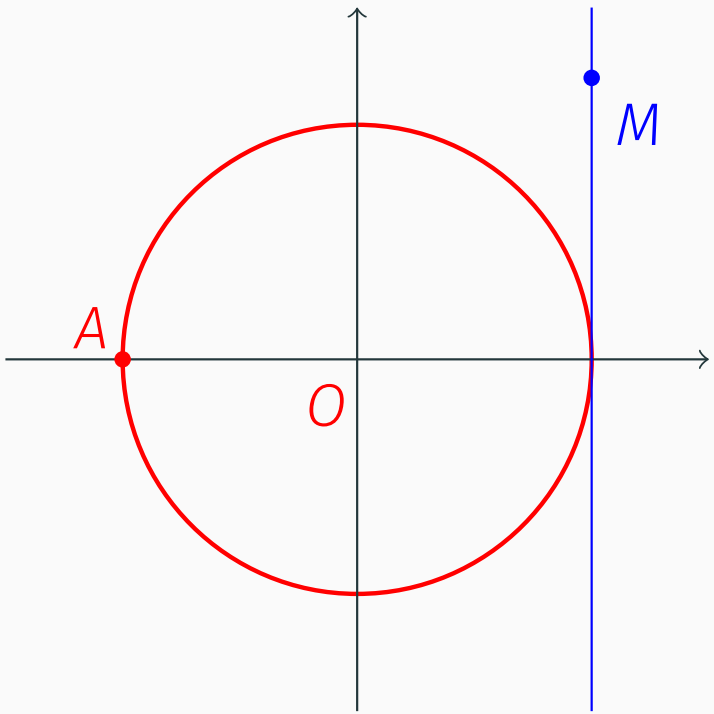
L'équation de Pythagore

Il s'agit de trouver les solutions de l'équation

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

Seules solutions entières : $(\pm 1, 0)$, $(0, \pm 1)$.

Solutions en nombres rationnels ?



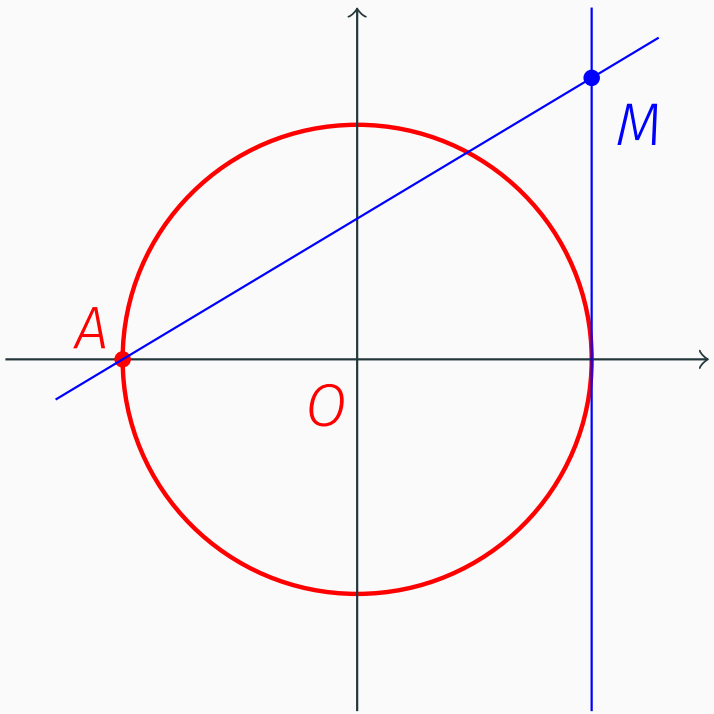
L'équation de Pythagore

Il s'agit de trouver les solutions de l'équation

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

Seules solutions entières : $(\pm 1, 0)$, $(0, \pm 1)$.

Solutions en nombres rationnels ?



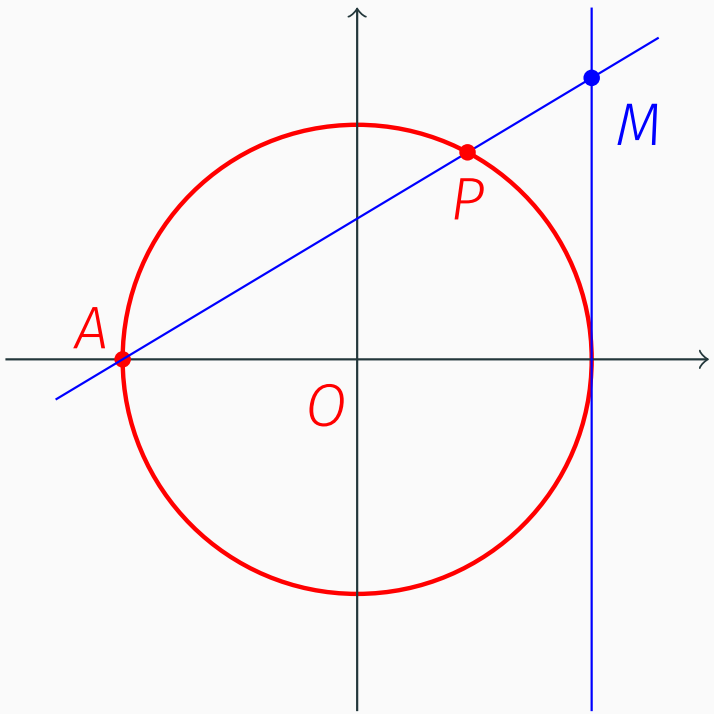
L'équation de Pythagore

Il s'agit de trouver les solutions de l'équation

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

Seules solutions entières : $(\pm 1, 0)$, $(0, \pm 1)$.

Solutions en nombres rationnels ?



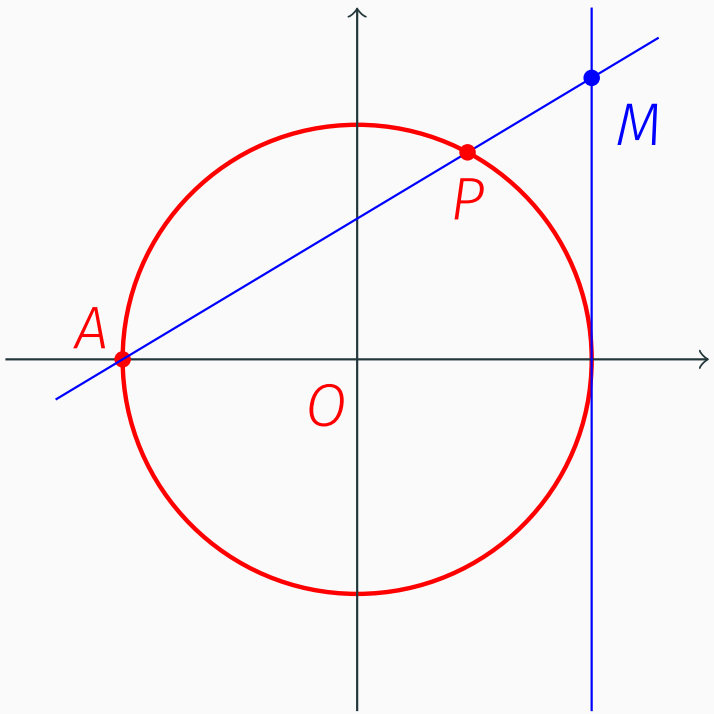
L'équation de Pythagore

Il s'agit de trouver les solutions de l'équation

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

Seules solutions entières : $(\pm 1, 0)$, $(0, \pm 1)$.

Solutions en nombres rationnels ?



Si M a pour coordonnées $(1, 2t)$, alors P a pour coordonnées (x, y) avec

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

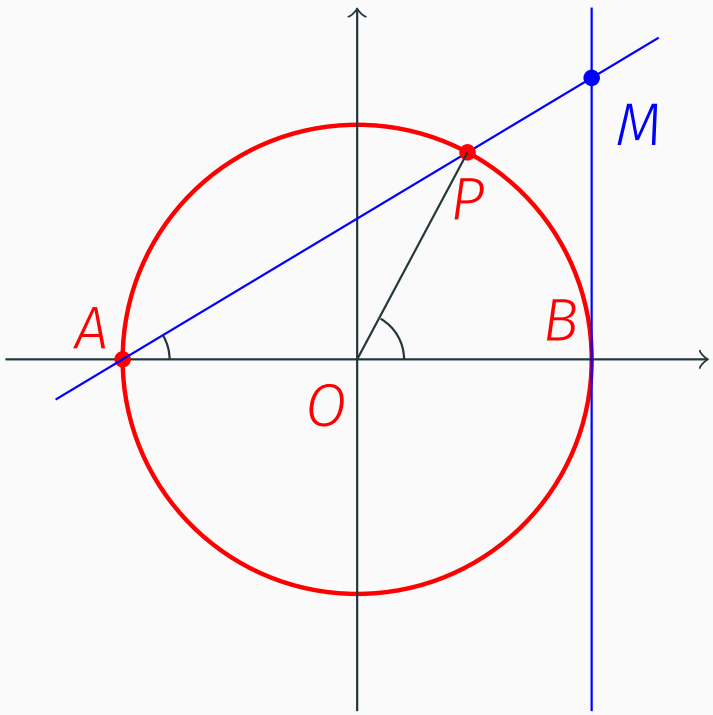
L'équation de Pythagore

Il s'agit de trouver les solutions de l'équation

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

Seules solutions entières : $(\pm 1, 0)$, $(0, \pm 1)$.

Solutions en nombres rationnels ?



Si M a pour coordonnées $(1, 2t)$, alors P a pour coordonnées (x, y) avec

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

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

Paramétrage rationnel des coniques

La procédure expliquée pour le cercle fonctionne pour *toute conique* (équation du second degré en deux variables) *pourvu* qu'il existe déjà une solution rationnelle.

Paramétrage rationnel des coniques

La procédure expliquée pour le cercle fonctionne pour *toute conique* (équation du second degré en deux variables) *pourvu* qu'il existe déjà une solution rationnelle.

Exemples :

- $x^2 + y^2 = -1$ — problème de signe
- $x^2 + y^2 = 3$ — problème modulo 4.

Paramétrage rationnel des coniques

La procédure expliquée pour le cercle fonctionne pour *toute conique* (équation du second degré en deux variables) *pourvu* qu'il existe déjà une solution rationnelle.

Exemples :

- $x^2 + y^2 = -1$ — problème de signe
- $x^2 + y^2 = 3$ — problème modulo 4.

Théorème (Hasse, 1921)

S'il n'y a pas de problème de signe ni de problème de congruence, alors il y a une solution rationnelle.

Le théorème de Hasse–Minkowski

Il y a un théorème général pour n'importe quelle équation de degré 2 en n'importe quel nombre de variables. Pour l'énoncer, il faut introduire les « corps p-adiques » qui sont des petits cousins du corps des nombres réels, mais où la notion de proximité (via la valeur absolue) est remplacée par des congruences faisant intervenir un nombre premier p.

Théorème (Hasse–Minkowski)

Si une forme quadratique $q(x, y, z, \dots)$ à coefficients dans $\mathbf{Q}$ a des solutions non triviales dans tous les corps p-adiques, ainsi que dans les réels, alors elle a une solution non triviale dans $\mathbf{Q}$.

Équations de degré 3 et plus

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.

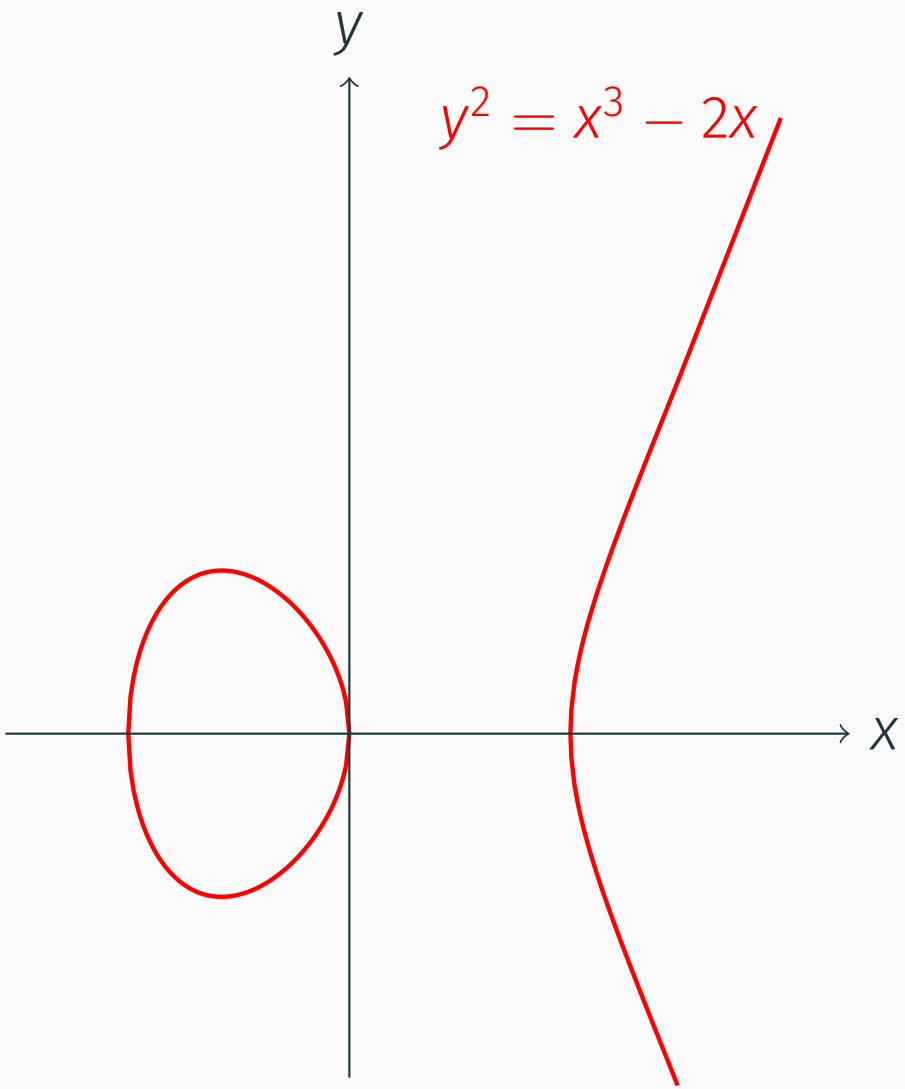
ΤΟΝ ὑπερβάντα τετράγωνον διελεῖν εἰς δύο τετραγώνους. ἐπιτετάχθω δὴ τὸ ιϛ διελεῖν εἰς δύο τετραγώνους. καὶ τετάχθω ὁ πρῶτος δυνάμεως μιᾶς. δεήσει ἄρα μονάδας ιϛ λείψει δυνάμεως μιᾶς ἴσας εἶναι τετραγώνῳ. πλάσσω τὸ τετράγωνον ἀπὸ ϛς. ὅσων δὴ ποτε λείψει τοσούτων μ̄ ὅσων ἐστὶν ἡ τοῦ ιϛ μ̄ πλευρά. ἔστω ϛς β λείψει μ̄ δ̄. αὐτὸς ἄρα ὁ τετράγωνος ἔσται δυνάμεων δ̄ μ̄ ιϛ λείψει ϛς 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 εἷς ιϛ εἰκοσοπέμπτων. ὁ δὲ ῥιδ εἰκοσοπέμπτων, καὶ οἱ δύο συντεθέντες ποιοῦσι υ εἰκοσόπεμπτα, ἤτοι μονάδας ιϛ. καὶ ἔστιν ἑκάτερος τετράγωνος.

OBSERVATIO DOMINI PETRI DE FERMAT.

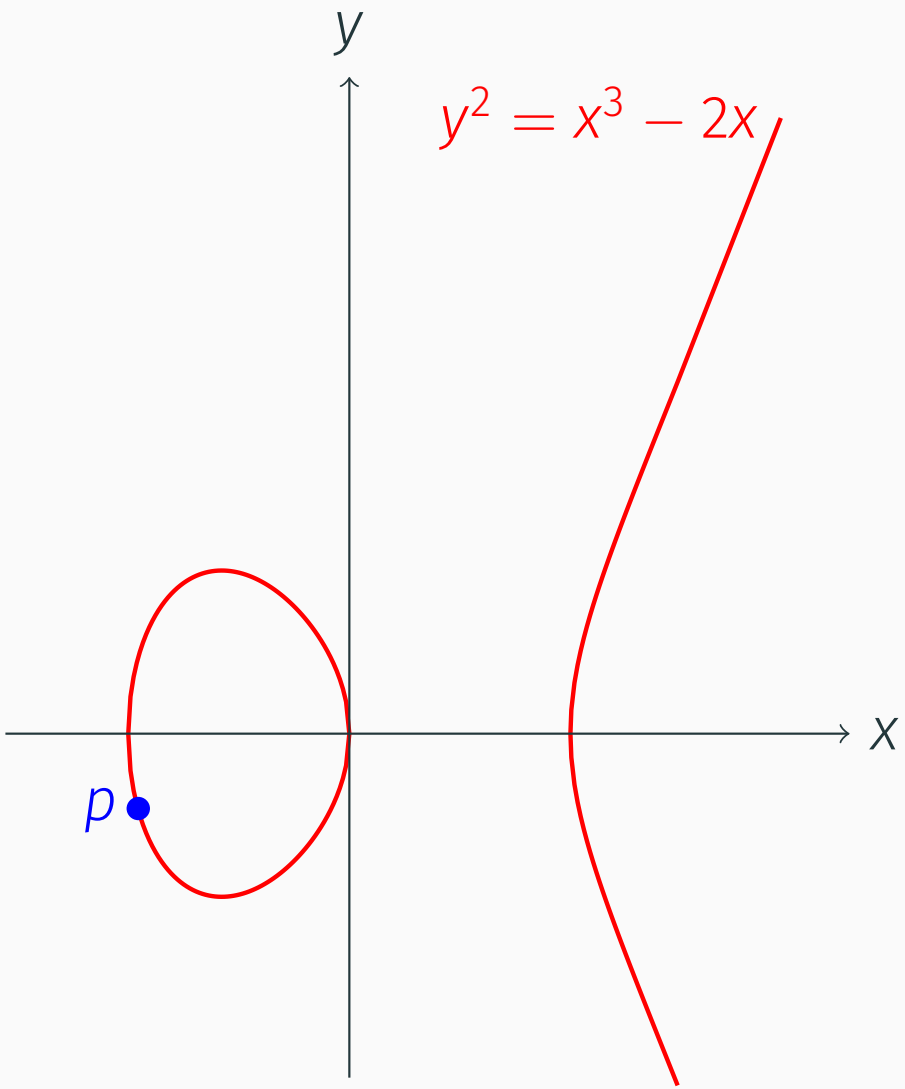
CVbum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum poteſtatem in duos eiuſdem nominis fas eſt diuidere cuius rei demonſtrationem mirabilem ſane detexi. Hanc marginis exiguitas non caperet.

Diophante, *Arithmétique*. Édition de 1670. Source : *Wikipedia*

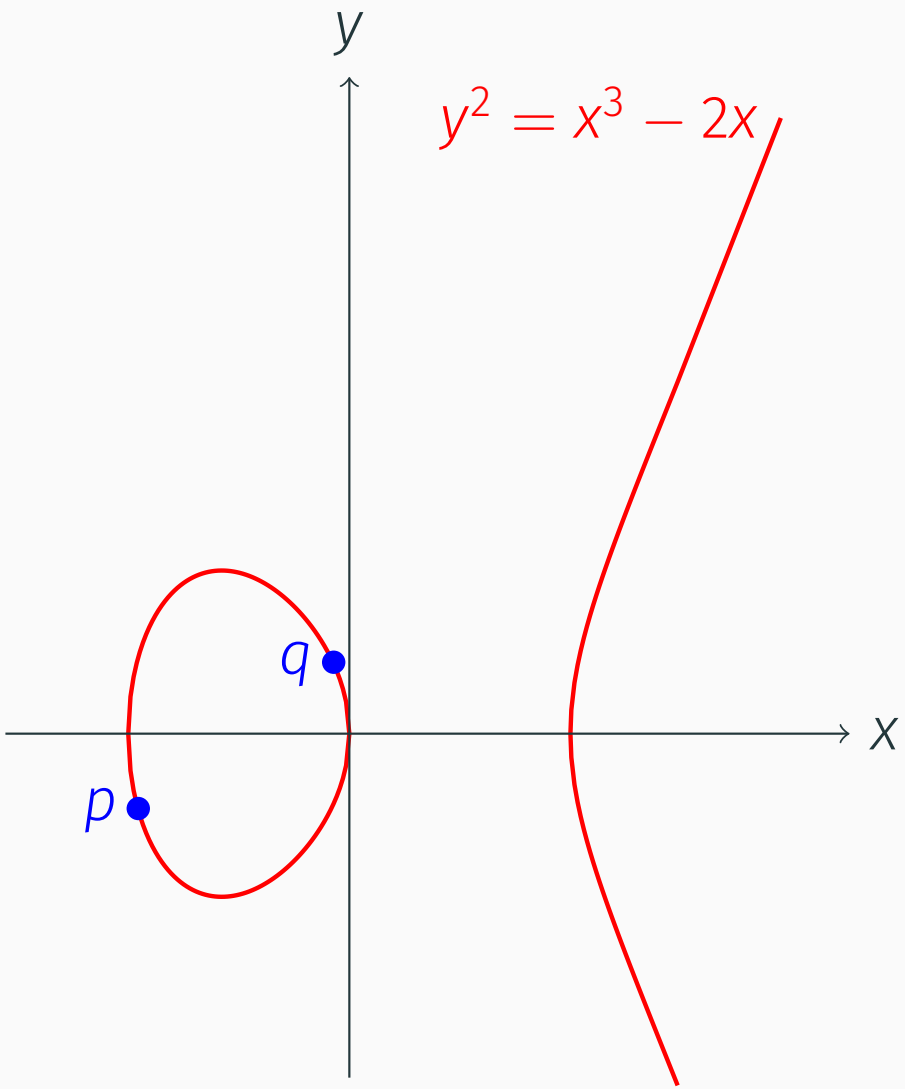
Une équation cubique



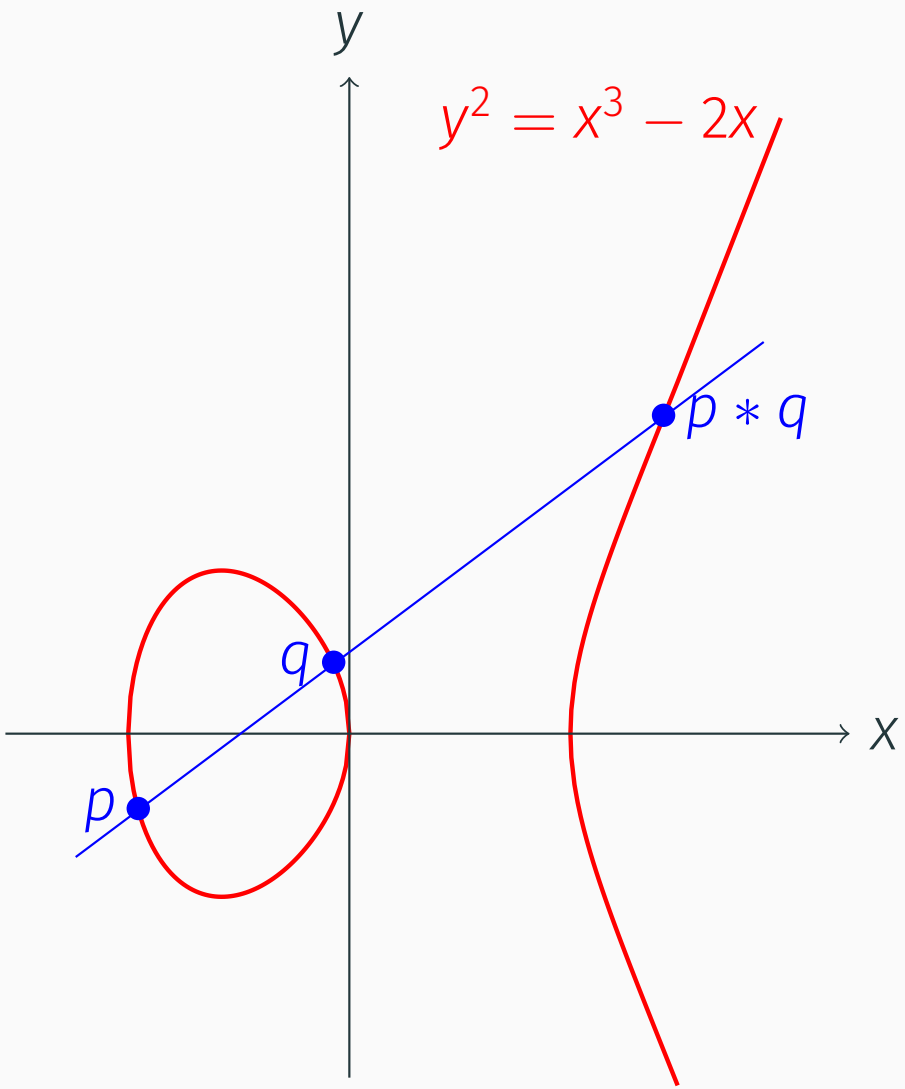
Une équation cubique



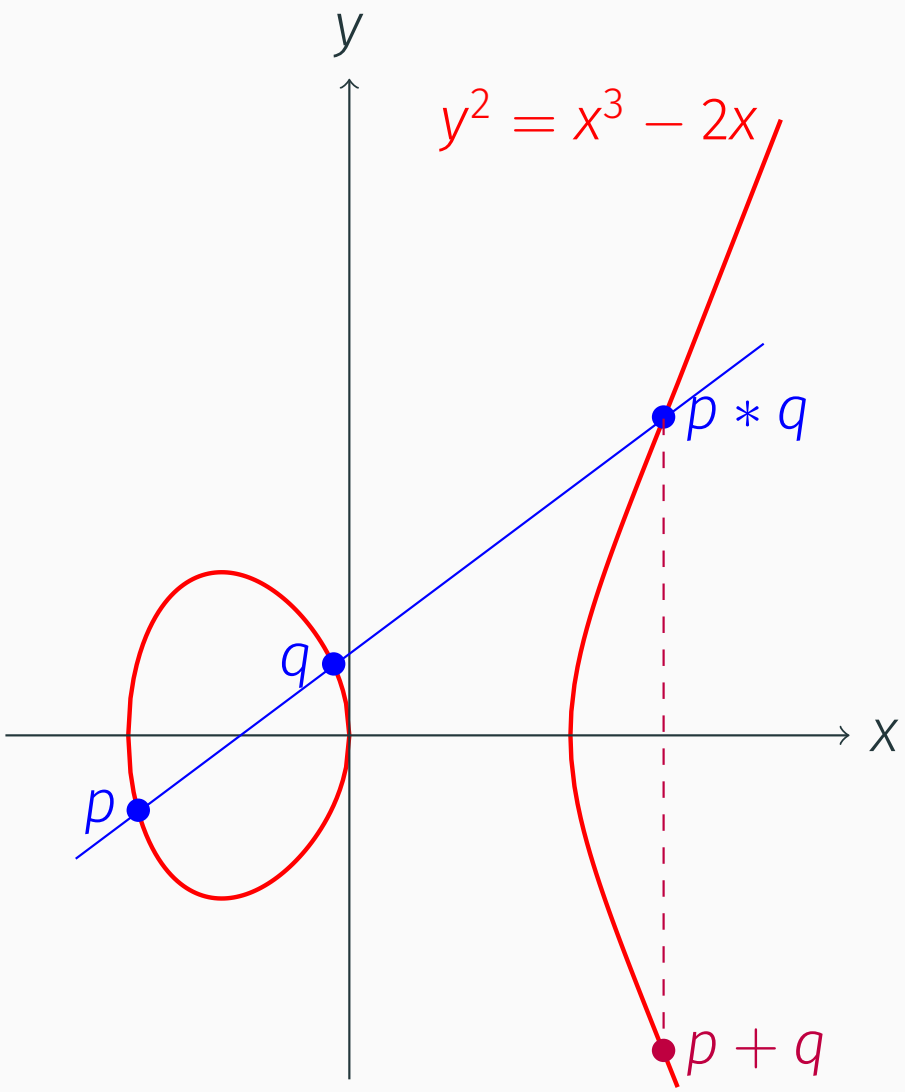
Une équation cubique



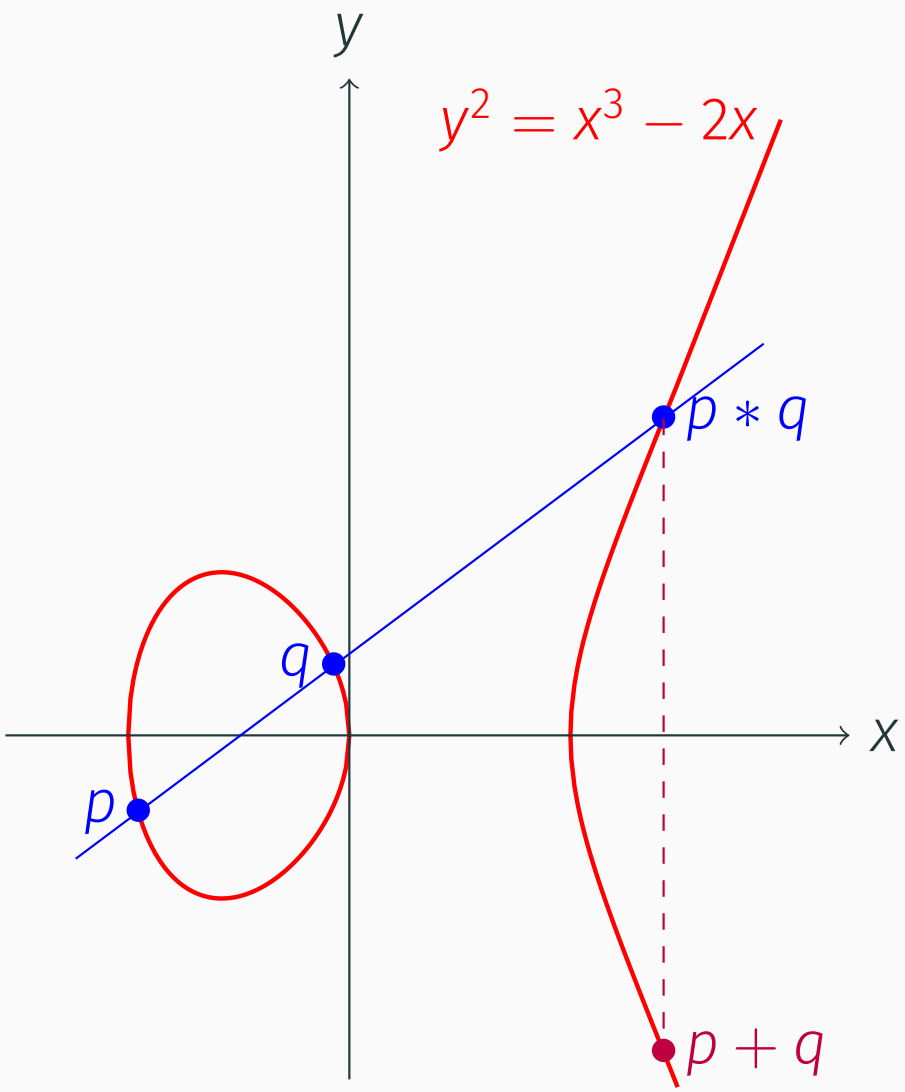
Une équation cubique



Une équation cubique



Une équation cubique



On définit ainsi une *loi de groupe* commutative sur l'ensemble des solutions rationnelles. L'élément neutre est un point « à l'infini ».

Courbes elliptiques

Ce sont les courbes définies par une équation cubique de la forme

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

Courbes elliptiques

Ce sont les courbes définies par une équation cubique de la forme

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

La condition sur le discriminant signifie que la cubique est *non singulière* : si (x,y) est un point singulier,

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

entraîne que $y = 0$ et x est racine double de $x^3 + ax + b$.

Courbes elliptiques

Ce sont les courbes définies par une équation cubique de la forme

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

La condition sur le discriminant signifie que la cubique est *non singulière* : si (x,y) est un point singulier,

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

entraîne que $y = 0$ et x est racine double de $x^3 + ax + b$.

Contrairement aux coniques, on ne peut pas les paramétrer par des fractions rationnelles.

Courbes elliptiques — Une autre conjecture de Poincaré

Considérons une courbe elliptique, donnée par équation cubique de la forme

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

a et b étant des nombres rationnels.

Théorème (Mordell, 1922)

Le groupe des solutions rationnelles est un groupe abélien de type fini.

Courbes elliptiques — Une autre conjecture de Poincaré

Considérons une courbe elliptique, donnée par équation cubique de la forme

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

a et b étant des nombres rationnels.

Théorème (Mordell, 1922)

Le groupe des solutions rationnelles est un groupe abélien de type fini.

Théorème (Siegel, 1929)

Il n'y a qu'un nombre fini de solutions entières.

Équations de degré supérieur

On considère maintenant une équation de degré au moins 4, définissant une courbe *non singulière*. Il est important de se placer dans le cadre de la *géométrie projective* et de tenir compte des singularités à l'infini, ou complexes.

Théorème (Faltings, 1983 ; conjecturé par Mordell)

Il n'y a qu'un nombre fini de solutions rationnelles.

Équations de degré supérieur

On considère maintenant une équation de degré au moins 4, définissant une courbe *non singulière*. Il est important de se placer dans le cadre de la *géométrie projective* et de tenir compte des singularités à l'infini, ou complexes.

Théorème (Faltings, 1983 ; conjecturé par Mordell)

Il n'y a qu'un nombre fini de solutions rationnelles.

Conséquence : pour tout entier $n \geqslant 4$, l'équation de Fermat n'a qu'un nombre fini de solutions.

Trichotomie géométrique

Jusqu'à présent, on a vu trois grandes classes d'équations :

- degré 1 ou 2 (coniques) : paramétrisations rationnelles, nombre parfois infini de solutions entières ;
- degré 3 (« courbes elliptiques ») : pas de paramétrisation des solutions, nombre parfois infini de solutions rationnelles, nombre fini de solutions entières ;
- degré 4 ou plus : nombre fini de solutions rationnelles.

Trichotomie géométrique

Jusqu'à présent, on a vu trois grandes classes d'équations :

- degré 1 ou 2 (coniques) : paramétrisations rationnelles, nombre parfois infini de solutions entières ;
- degré 3 (« courbes elliptiques ») : pas de paramétrisation des solutions, nombre parfois infini de solutions rationnelles, nombre fini de solutions entières ;
- degré 4 ou plus : nombre fini de solutions rationnelles.

La bonne façon de comprendre cette trichotomie consiste à regarder les solutions complexes qui forment une surface de Riemann. La distinction est alors

- genre 0 (sphère de Riemann, courbure > 0) ;
- genre 1 (courbure nulle) ;
- genre 2 ou plus (courbure < 0).

En dimension plus grande ?

Pour les systèmes d'équations dont la géométrie est de plus grande dimension, la situation est largement ouverte.

En dimension plus grande ?

Pour les systèmes d'équations dont la géométrie est de plus grande dimension, la situation est largement ouverte.

On se limite au cas de systèmes d'équations définissant une variété algébrique complexe projective et lisse.

L'analogue de la condition « genre $\geqslant 2$ » s'appelle variété de type général.

En dimension plus grande ?

Pour les systèmes d'équations dont la géométrie est de plus grande dimension, la situation est largement ouverte.

On se limite au cas de systèmes d'équations définissant une variété algébrique complexe projective et lisse.

L'analogue de la condition « genre $\geqslant 2$ » s'appelle variété de type général.

Une conjecture de Lang affirme qu'alors les solutions rationnelles sont contenues dans une sous-variété algébrique stricte. Autrement dit, elles vérifient une condition algébrique supplémentaire !

En dimension plus grande ?

Pour les systèmes d'équations dont la géométrie est de plus grande dimension, la situation est largement ouverte.

On se limite au cas de systèmes d'équations définissant une variété algébrique complexe projective et lisse.

L'analogue de la condition « genre $\geqslant 2$ » s'appelle variété de type général.

Une conjecture de Lang affirme qu'alors les solutions rationnelles sont contenues dans une sous-variété algébrique stricte. Autrement dit, elles vérifient une condition algébrique supplémentaire !

Seul (?) cas connu : sous-variétés de variétés abéliennes (Faltings, 1991).

Une conjecture d'Euler

Par analogie avec l'équation de Fermat, Euler a conjecturé en 1769 que l'équation diophantienne :

$$a^4 + b^4 + c^4 = d^4$$

n'avait pas de solutions en nombre entiers > 0, ainsi qu'une propriété similaire en degré supérieur.

Théorème (Elkies 1987)

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4$$

La démonstration d'Elkies repose sur la compréhension géométrique de la surface d'équation $x^4 + y^4 + z^4 = 1$, écrite comme une famille de courbes elliptiques, et la découverte de points sur certaines d'entre elles.

Une conjecture d'Euler

Théorème (Frye, 1987)

$$95800^4 + 217519^4 + 414560^4 = 422481^4$$

La preuve de Frye repose une recherche par ordinateur intensive, facilitée par l'observation qu'un certain nombre de congruences doivent être vérifiées.

C'est le plus petit contre-exemple.

Décider une équation diophantienne

Le 10e problème de Hilbert

David Hilbert, 1900, Congrès international des mathématiciens :

Le 10e problème de Hilbert

David Hilbert, 1900, Congrès international des mathématiciens :

> *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.

Le 10e problème de Hilbert

David Hilbert, 1900, Congrès international des mathématiciens :

> *De la possibilité de résoudre une équation diophantienne.*
>
> On donne une équation diophantienne en un nombre quelconque d'inconnues et à coefficients entiers rationnels : on demande de trouver une méthode par laquelle, au moyen d'un nombre fini d'opérations, on pourra distinguer si l'équation est résoluble en nombres entiers rationnels.

Le problème de décision (Hilbert, 1928)

En 1928, Hilbert généralise son 10e problème et énoncé le problème de décision (Entscheidungsproblem) : il s'agit de prouver (ou d'infirmer) l'existence d'un algorithme qui résout tout problème mathématique (convenablement formalisé, en logique du premier ordre).

Le problème de décision (Hilbert, 1928)

En 1928, Hilbert généralise son 10e problème et énoncé le problème de décision (Entscheidungsproblem) : il s'agit de prouver (ou d'infirmer) l'existence d'un algorithme qui résout tout problème mathématique (convenablement formalisé, en logique du premier ordre).

1936 : Gödel, Turing, Church prouvent qu'un tel algorithme n'existe pas.

Mais pour les équations diophantiennes ?

Si le problème général de la décision n'a pas de solution, on peut encore espérer que le 10e problème de Hilbert a une réponse positive.

Mais pour les équations diophantiennes ?

Si le problème général de la décision n'a pas de solution, on peut encore espérer que le 10e problème de Hilbert a une réponse positive.

Théorème (Matyasevich, 1970)

Il n'existe pas d'algorithme qui, étant donné une équation diophantienne arbitraire, dise si elle possède une solution en nombres entiers, ou non.

Mais pour les équations diophantiennes ?

Si le problème général de la décision n'a pas de solution, on peut encore espérer que le 10e problème de Hilbert a une réponse positive.

Théorème (Matyasevich, 1970)

Il n'existe pas d'algorithme qui, étant donné une équation diophantienne arbitraire, dise si elle possède une solution en nombres entiers, ou non.

Version forte : Il existe un polynôme

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

en 10 variables telle qu'aucun algorithme ne puisse dire, étant donné un entier $a \in \mathbb{Z}$, si l'équation $f(a, x_1, \ldots, x_9) = 0$ possède une solution dans $\mathbb{Z}^9$ ou pas.

Mais pour les équations diophantiennes ?

Si le problème général de la décision n'a pas de solution, on peut encore espérer que le 10e problème de Hilbert a une réponse positive.

Théorème (Matyasevich, 1970)

Il n'existe pas d'algorithme qui, étant donné une équation diophantienne arbitraire, dise si elle possède une solution en nombres entiers, ou non.

Version forte : Il existe un polynôme

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

en 10 variables telle qu'aucun algorithme ne puisse dire, étant donné un entier $a \in \mathbf{Z}$, si l'équation $f(a, x_1, \ldots, x_9) = 0$ possède une solution dans $\mathbf{Z}^9$ ou pas.

Pour les solutions rationnelles : la question est ouverte !

Et pour les équations en deux variables ?

Revenons donc aux équations en deux variables définissant une courbe non singulière.

Et pour les équations en deux variables ?

Revenons donc aux équations en deux variables définissant une courbe non singulière.

En genre 0, le théorème de Hasse-Minkowski permet de décider effectivement si l'équation possède une solution rationnelle ou pas. Le point est qu'il n'y a qu'un nombre fini de congruences à vérifier.

Et pour les équations en deux variables ?

Revenons donc aux équations en deux variables définissant une courbe non singulière.

En genre 0, le théorème de Hasse-Minkowski permet de décider effectivement si l'équation possède une solution rationnelle ou pas. Le point est qu'il n'y a qu'un nombre fini de congruences à vérifier.

En genre 1, on a une majoration de la taille d'une solution entière (A. Baker, $\leqslant$ 1970). Pour les solutions rationnelles, il existe un procédé qui, en pratique, fournira tôt ou tard des générateurs du groupe des solutions (*cf.* Tate, 1974) mais c'est encore une conjecture (« finitude du groupe de Tate-Shafarevich »).

Et pour les équations en deux variables ?

Revenons donc aux équations en deux variables définissant une courbe non singulière.

En genre 0, le théorème de Hasse-Minkowski permet de décider effectivement si l'équation possède une solution rationnelle ou pas. Le point est qu'il n'y a qu'un nombre fini de congruences à vérifier.

En genre 1, on a une majoration de la taille d'une solution entière (A. Baker, $\leqslant$ 1970). Pour les solutions rationnelles, il existe un procédé qui, en pratique, fournira tôt ou tard des générateurs du groupe des solutions (*cf.* Tate, 1974) mais c'est encore une conjecture (« finitude du groupe de Tate-Shafarevich »).

En genre $\geqslant 2$, obtenir une version effective de la conjecture de Mordell est une question complètement ouverte.

La conjecture ABC

Conjecture (Oesterlé, Masser, 1985)

Pour tout $\theta > 1$, il existe $K_\theta > 0$ de sorte que l'on ait :

Si A, B, C sont trois entiers premiers entre eux tels que $A + B = C$, alors

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

Le *radical* d'un entier (ici ABC) est le produit des nombres premiers qui le divisent. – Autrement dit, cette conjecture affirme que les multiplicités des facteurs premiers de A, B, C ne sont pas trop grandes.

La conjecture ABC

Conjecture (Oesterlé, Masser, 1985)

Pour tout $\theta > 1$, il existe $K_\theta > 0$ de sorte que l'on ait :

Si A, B, C sont trois entiers premiers entre eux tels que $A + B = C$, alors

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

Le *radical* d'un entier (ici ABC) est le produit des nombres premiers qui le divisent. – Autrement dit, cette conjecture affirme que les multiplicités des facteurs premiers de A, B, C ne sont pas trop grandes.

Record (Reyssat, 1987) :

$$2 + 3^{10} \times 109 = 23^5, \qquad \theta(a, b, c) := \frac{\log(\max(a, b, c))}{\log(\operatorname{rad}(abc))} \approx 1{,}63$$

Fermat comme conséquence de la conjecture ABC

Soit une solution (x, y, z) non triviale $(xyz \neq 0)$ de l'équation de Fermat $x^n + y^n = z^n$. On peut supposer x, y, z premiers entre eux.

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

Fermat comme conséquence de la conjecture ABC

Soit une solution (x, y, z) non triviale ($xyz \neq 0$) de l'équation de Fermat $x^n + y^n = z^n$. On peut supposer x, y, z premiers entre eux.

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

Comme $\mathrm{rad}(x^n y^n z^n) = \mathrm{rad}(xyz)$, si la conjecture ABC est vraie, on a

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

D'autre part, il est évident que
$\mathrm{rad}(xyz) \leqslant |x|\ |y|\ |z| \leqslant \max(|x|, |y|, |z|)^3$. On a donc

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

d'où, si $n > 3\theta$,

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

Fermat comme conséquence de la conjecture ABC

Soit une solution (x, y, z) non triviale ($xyz \neq 0$) de l'équation de Fermat $x^n + y^n = z^n$. On peut supposer x, y, z premiers entre eux.

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

Comme $\mathrm{rad}(x^n y^n z^n) = \mathrm{rad}(xyz)$, si la conjecture ABC est vraie, on a

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

D'autre part, il est évident que
$\mathrm{rad}(xyz) \leqslant |x|\ |y|\ |z| \leqslant \max(|x|, |y|, |z|)^3$. On a donc

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

d'où, si $n > 3\theta$,

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

Ainsi, on contrôle les solutions de l'équation de Fermat en

Fermat comme conséquence de la conjecture ABC

Pour θ donné et $n > 3\theta$, l'inégalité

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

prouve que l'équation de Fermat de degré n n'a qu'un nombre *fini* de solutions.

Les trouver explicitement demanderait une information sur la constante K_θ — et peut-être une longue recherche.

Fermat comme conséquence de la conjecture ABC

Pour θ donné et $n > 3\theta$, l'inégalité

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

prouve que l'équation de Fermat de degré n n'a qu'un nombre *fini* de solutions.

Les trouver explicitement demanderait une information sur la constante K_θ — et peut-être une longue recherche.

Quand n est assez grand (dépendant de la constante K_θ), cette inégalité entraîne que $|x|$, $|y|$, $|z|$ sont 0 ou 1, et cela prouve le théorème de Fermat !

La conjecture ABC pour les polynômes

Théorème (Stothers, 1981 ; Mason, 1984)

Soit $A, B, C \in \mathbf{C}[t]$ trois polynômes premiers entre eux, non tous constants, tels que $A + B = C$. Alors

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

Ici, $\nu(ABC)$ est le nombre de racines complexes (sans multiplicité) du polynôme ABC.

La conjecture ABC pour les polynômes : démonstration

On pose $D = AB' - A'B = AC' - A'C = CB' - C'B$.

La conjecture ABC pour les polynômes : démonstration

On pose $D = AB' - A'B = AC' - A'C = CB' - C'B$.

On a $D \neq 0$, et $\deg(D) \leqslant \deg(A) + \deg(B) - 1$.

La conjecture ABC pour les polynômes : démonstration

On pose $D = AB' - A'B = AC' - A'C = CB' - C'B$.

On a $D \neq 0$, et $\deg(D) \leqslant \deg(A) + \deg(B) - 1$.

Si x est une racine de multiplicité m de A, B ou C,
c'est une racine de multiplicité $\geqslant m - 1$ de D, donc

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

La conjecture ABC pour les polynômes : démonstration

On pose $D = AB' - A'B = AC' - A'C = CB' - C'B$.

On a $D \neq 0$, et $\deg(D) \leqslant \deg(A) + \deg(B) - 1$.

Si x est une racine de multiplicité m de A, B ou C,
c'est une racine de multiplicité $\geqslant m - 1$ de D, donc

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

On a donc $\deg(C) \leqslant \nu(ABC) - 1$,
et de même pour $\deg(A)$, $\deg(B)$.

Application à l'irrationalité géométrique

Grâce au théorème de Stothers-Mason, la même preuve que ABC $\Rightarrow$ Fermat *démontre* que les solutions de l'équation de Fermat ($n \geqslant 3$) ne sont pas paramétrables par des fonctions rationnelles.

Application à l'irrationalité géométrique

Grâce au théorème de Stothers-Mason, la même preuve que ABC $\Rightarrow$ Fermat *démontre* que les solutions de l'équation de Fermat ($n \geqslant 3$) ne sont pas paramétrables par des fonctions rationnelles.

Si $P^n + Q^n = R^n$, pour trois polynômes $P, Q, R \in \mathbf{C}[t]$, premiers entre eux, on a

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

donc $n < 3$ si P, Q, R ne sont pas tous constants.

ABC $\Rightarrow$ Mordell

Théorème (Elkies, 1991)

Si la conjecture ABC est vraie, la version « effective » de la conjecture de Mordell l'est aussi : on peut donner une borne explicite pour la taille des solutions.

Principe : Construire (Belyĭ) une fonction rationnelle ϕ de x et y dont la restriction à la courbe est « non ramifiée » sauf au-dessus de $0, 1, \infty$.

ABC $\Rightarrow$ Mordell

Théorème (Elkies, 1991)

Si la conjecture ABC est vraie, la version « effective » de la conjecture de Mordell l'est aussi : on peut donner une borne explicite pour la taille des solutions.

Principe : Construire (Belyĭ) une fonction rationnelle ϕ de x et y dont la restriction à la courbe est « non ramifiée » sauf au-dessus de $0, 1, \infty$.

Appliquer la conjecture ABC à $\phi(P) + (1 - \phi(P)) = 1$, et conclure.

Mordell $\to$ ABC (effectivement)

On peut renverser les arguments :

Théorème (Moret-Bailly, Szpiro, 1990)

Une version effective de la conjecture de Mordell implique la conjecture ABC (avec un exposant plus grand que $1 + \varepsilon$*).*

Démontrer la conjecture ABC ?

17 septembre 2012, New York Times :

A Possible Breakthrough in Explaining a Mathematical Riddle

Démontrer la conjecture ABC ?

17 septembre 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. »

Démontrer la conjecture ABC ?

17 septembre 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. »

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