Donner une forme aux nombres
Une aventure bimillénaire

Antoine Chambert-Loir

Université Paris-Sud

13 juin 2013

Équations en tout genre

Équations *diophantiennes* :

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

Équations en tout genre

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.

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 de degré 1

Un vieux problème (III-V^{e} s. ap. J.-C.) :

Équations de degré 1

Un vieux problème (III-V^{e} 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-V^{e} 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

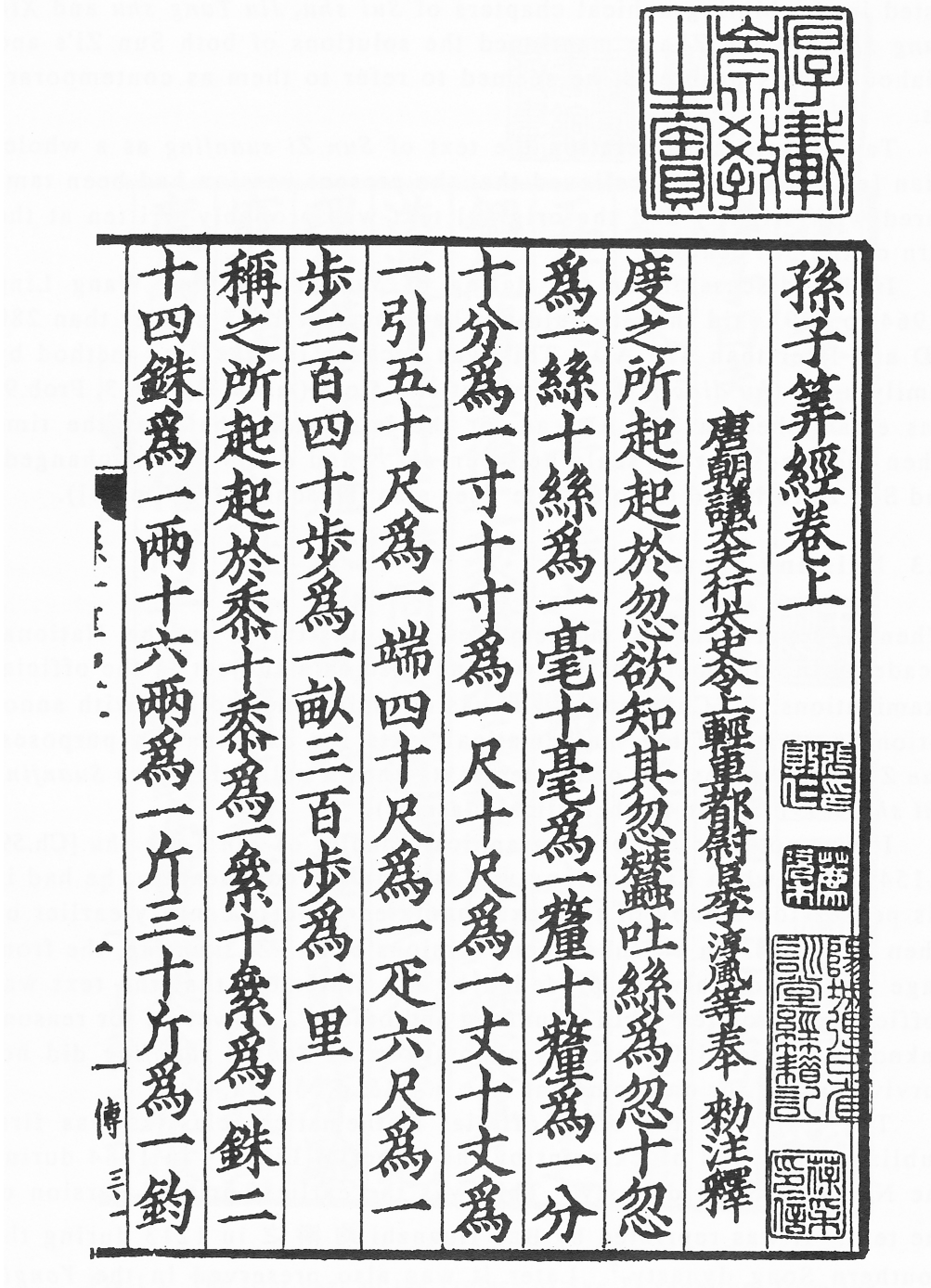
Un vieux problème (III-V^{e} s. ap. J.-C.) :

> 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*.



孫子算經卷上

唐朝議大夫行太史令上輕車都尉臣李淳風等奉 勅注釋

度之所起起於忽欲知其忽蠛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 Suànjīng,
reproduction d'une page d'une édition de la dynastie Qing

Source : *Wikipedia*

Le problème chinois

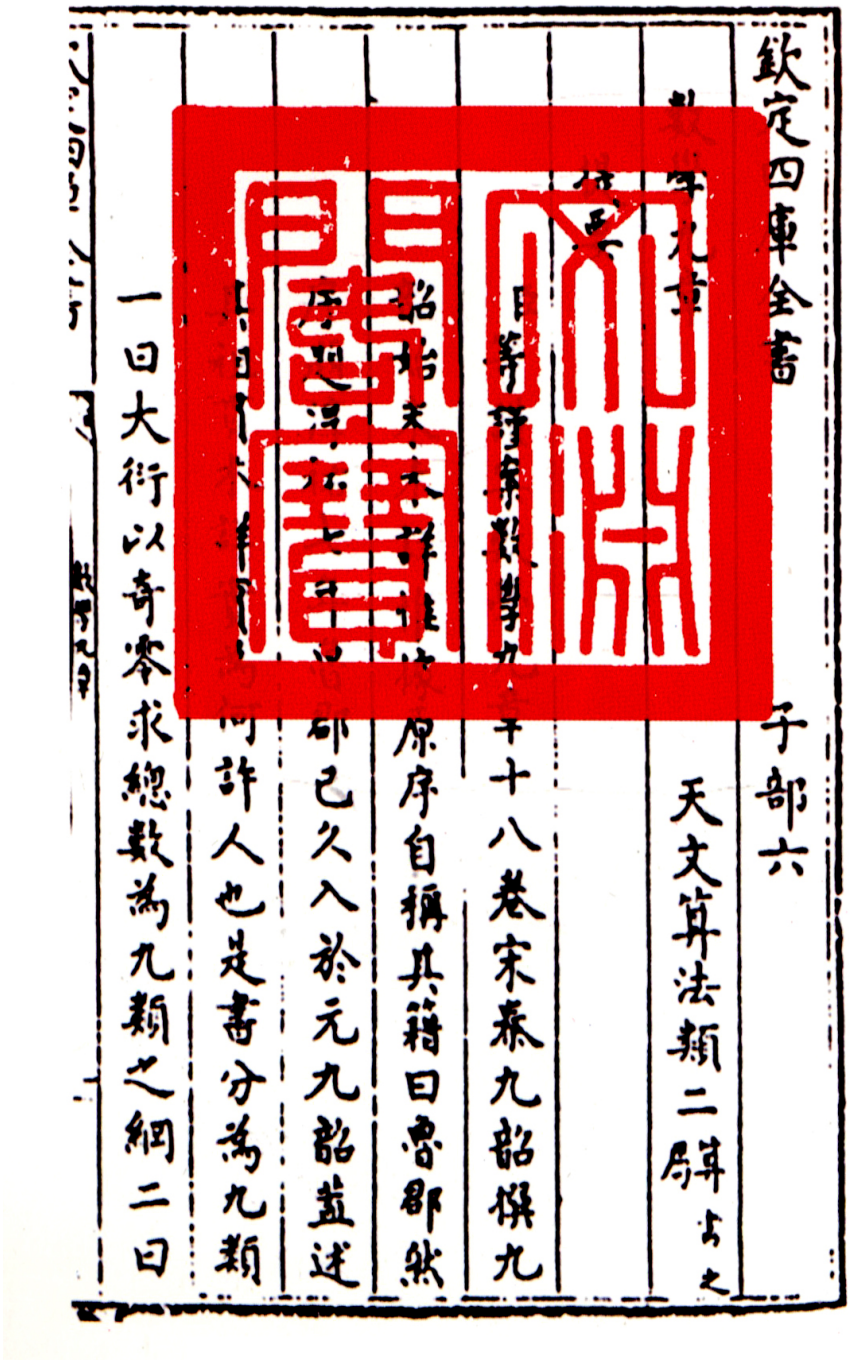
Ce genre d'exercices a ensuite été reproduit dans d'autres manuels, comme le

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, XIX^{e} s.,

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


欽定四庫全書

子部六

天文算法類二算之

十八卷宋秦九韶撰九

原序自稱其藉曰書郡然

郡已久入於元九韶益述

何許人也是書分為九類

一曰大衍以奇零求總數為九類之細二曰

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 $105 = 3 \times 5 \times 7$.

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
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

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 ἦσαν ταῦροι πλήθεσι βριθόμενοι
συμμετρίης τοιῆσδε τετευχότες· ἀργότριχας μέν
κυανέων ταύρων ἡμίσει ἠδὲ τριτῳ
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
ἵστανθ' ἀμβολάδην ἓξ ἑνὸς ἀρχόμενοι
σχῆμα τελειοῦντες τὸ τρικράσπεδον οὔτε προσόντων
ἀλλοχρόων ταύρων οὔτ' ἐπιλειπομένων.
ταῦτα συνεξευρὼν καὶ ἑνὶ 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

L'équation de Brahmagupta (Pell-Fermat)

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)

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 $(3, 2)$, $(17, 12)$,...

L'équation de Brahmagupta (Pell-Fermat)

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 $(3, 2)$, $(17, 12)$,...

Brahmagupta (628 ap. J.C.) : si (x, y) et (x', y') sont des solutions, on peut en construire une troisième (x'', y'') par la formule :

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

L'équation de Brahmagupta (Pell-Fermat)

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 $(3, 2)$, $(17, 12)$,...

Brahmagupta (628 ap. J.C.) : 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.

L'équation de Brahmagupta (Pell-Fermat)

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 $(3, 2)$, $(17, 12)$,...

Brahmagupta (628 ap. J.C.) : 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.

Explication moderne : on écrit

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

la *norme* du nombre quadratique $x + \sqrt{n}y$ et on observe que

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

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 : $(\pm 1, 0), (0, \pm 1)$.

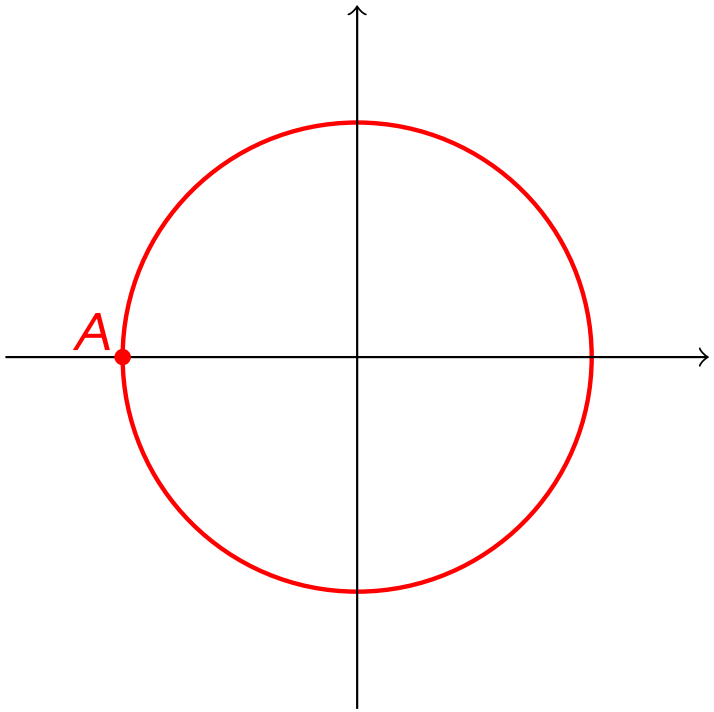
L'équation de Pythagore

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 ?



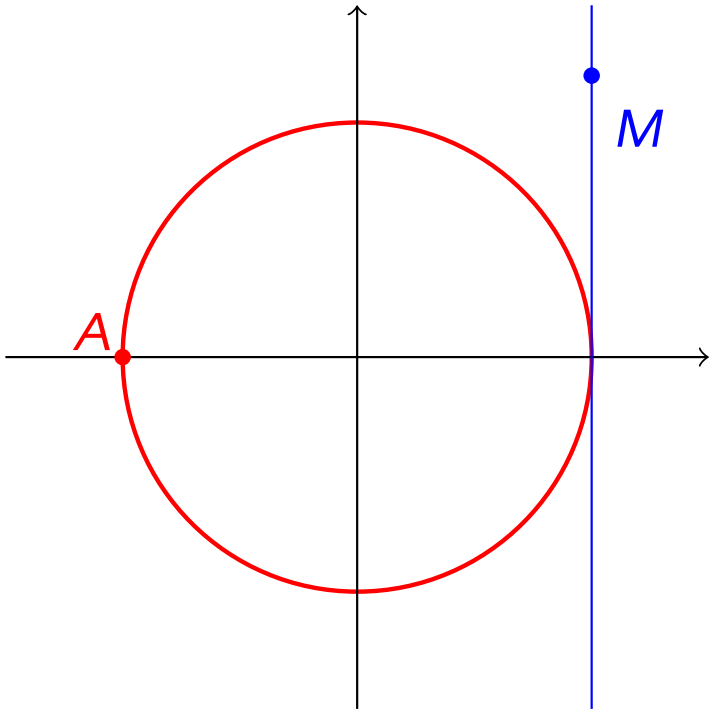
L'équation de Pythagore

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 ?



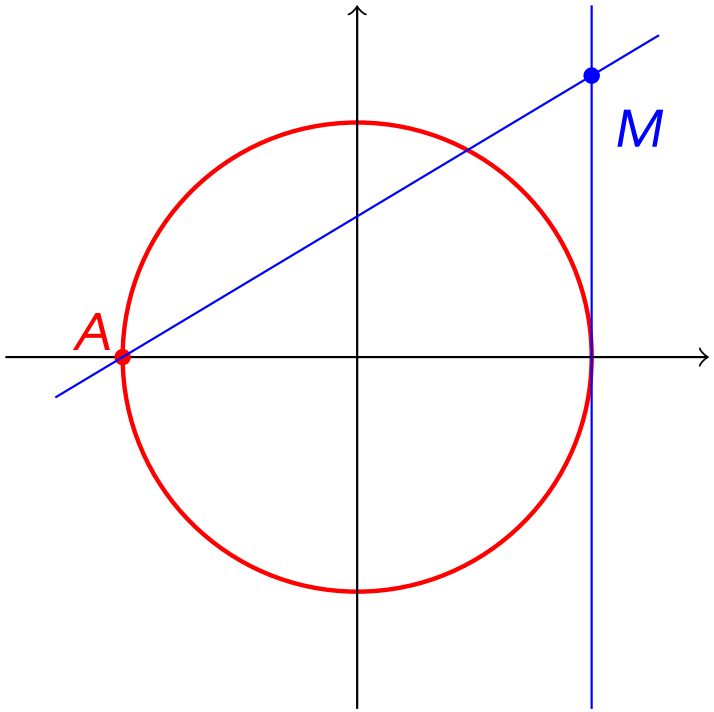
L'équation de Pythagore

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 ?



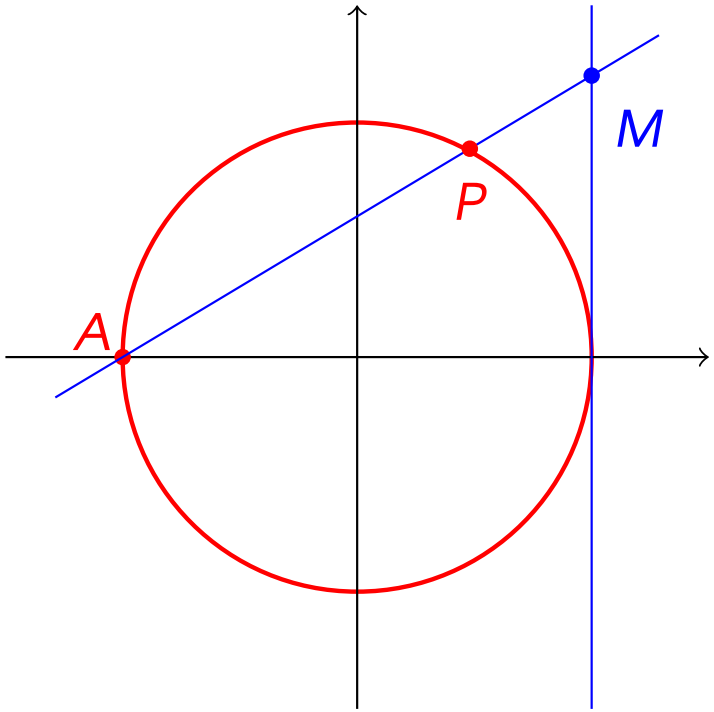
L'équation de Pythagore

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 ?



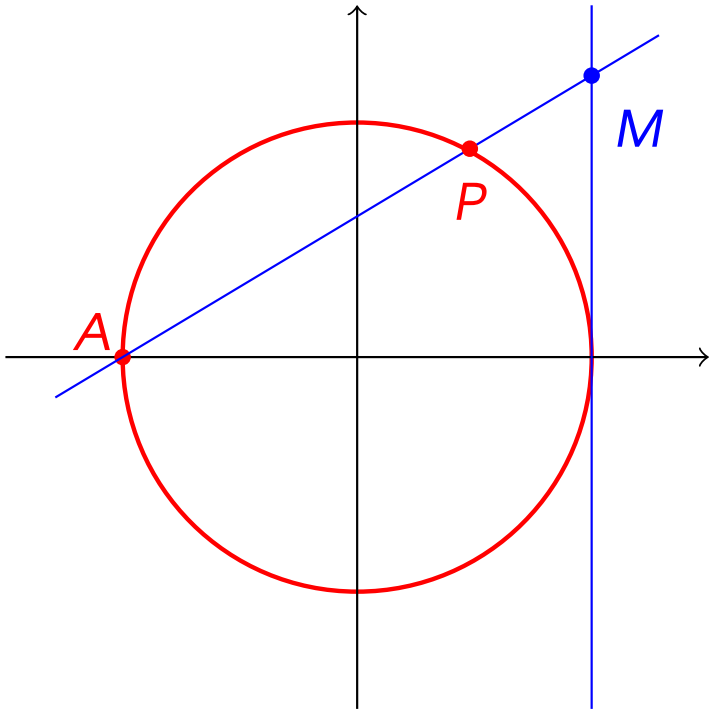
L'équation de Pythagore

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 $(1, t)$,
P a pour coordonnées (x, y) avec

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

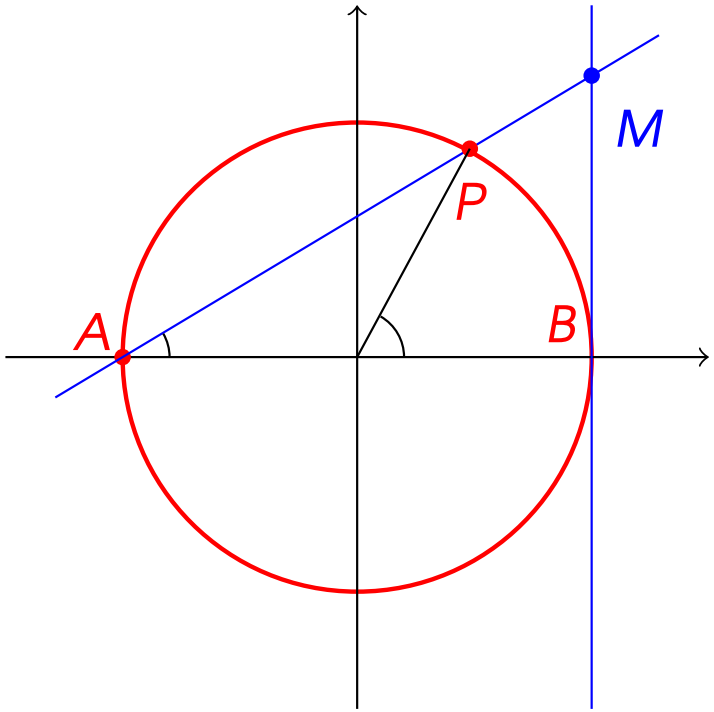
L'équation de Pythagore

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 $(1, t)$,
P a pour coordonnées (x, y) avec

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

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

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.

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.

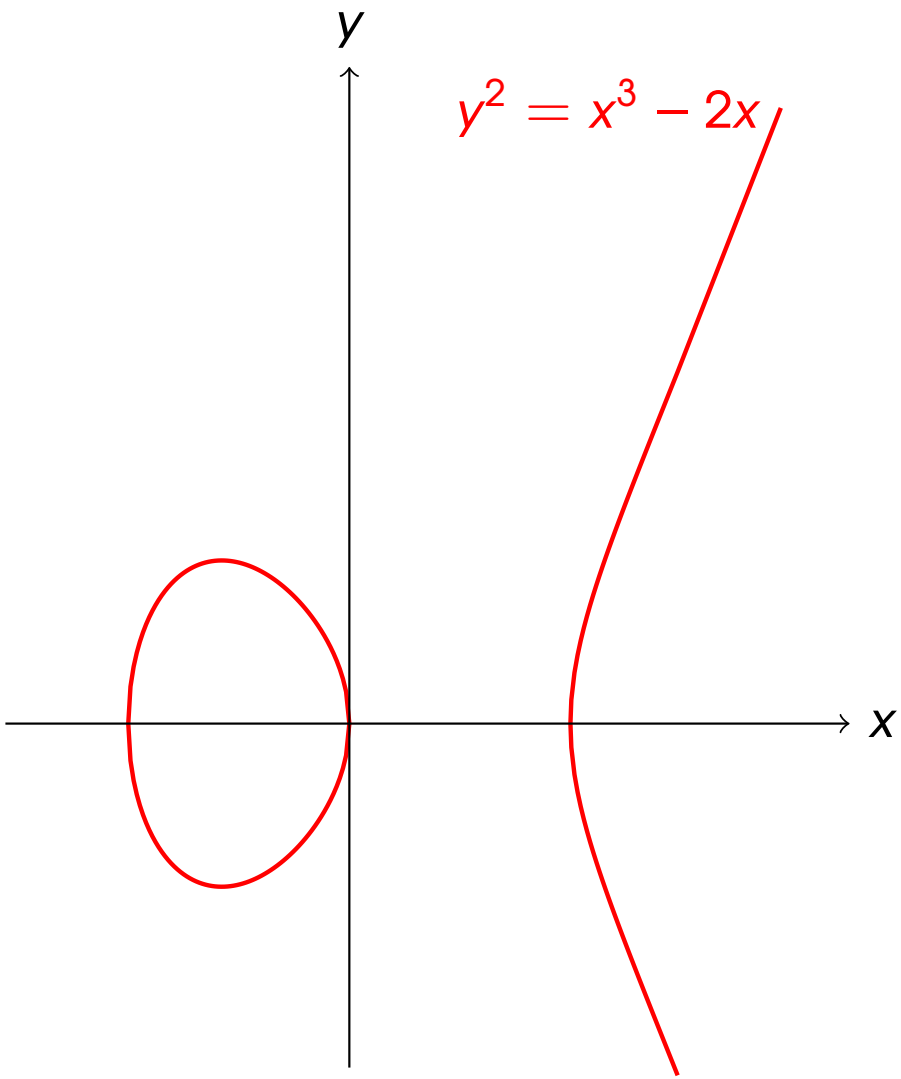
ΤΟΝ ὁπταχθέντα τετράγωνον διελεῖν εἰς δύο τετραγώνους. ἐπιτετάχθω δὴ τ ις διελεῖν εἰς δύο τετραγώνους. καὶ τετάχθω ὁ πρῶτος δυνάμεως μιᾶς. δήσει ἄρα μονάδας ις λείψει δυνάμεως μιᾶς ἴσας ἑνὶ τετραγώνῳ. πλάσω τ τετράγωνον ἀπὸ ςς. ὅσων δή ποτε λείψει τοσούτων μ ὅσων ὁ πλευρὰ ἔστω ςς β λείψει μ δ. αὐτὸς ἄρα ὁ τετράγωνος ἔσται δυνάμεων δ μ ις λείψει ςς ις. ταῦτα ἴσα μονάσι ις λείψει δυνάμεως μιᾶς. κοινὴ προσκείσθω ἡ λεῖψις, καὶ ἀπὸ ὁμοίων ὅμοια. δυνάμεις ἄρα ε ἴσαι ἀριθμοῖς ις. καὶ γίνεται ὁ ἀριθμὸς ις. πέμπτων. ἔσται ὁ μβ ος εἰκοσοπέμπτων. ὁ δὲ ρμδ εἰκοσοπέμπτων, ἃ οἱ δύο συντεθέντες ποιοῦσι υ εἰκοσόπεμπτα, ἥτοι μονάδας ις. καὶ ἔστιν ἑκάτερος τετράγωνος.

OBSERVATIO DOMINI PETRI DE FERMAT.

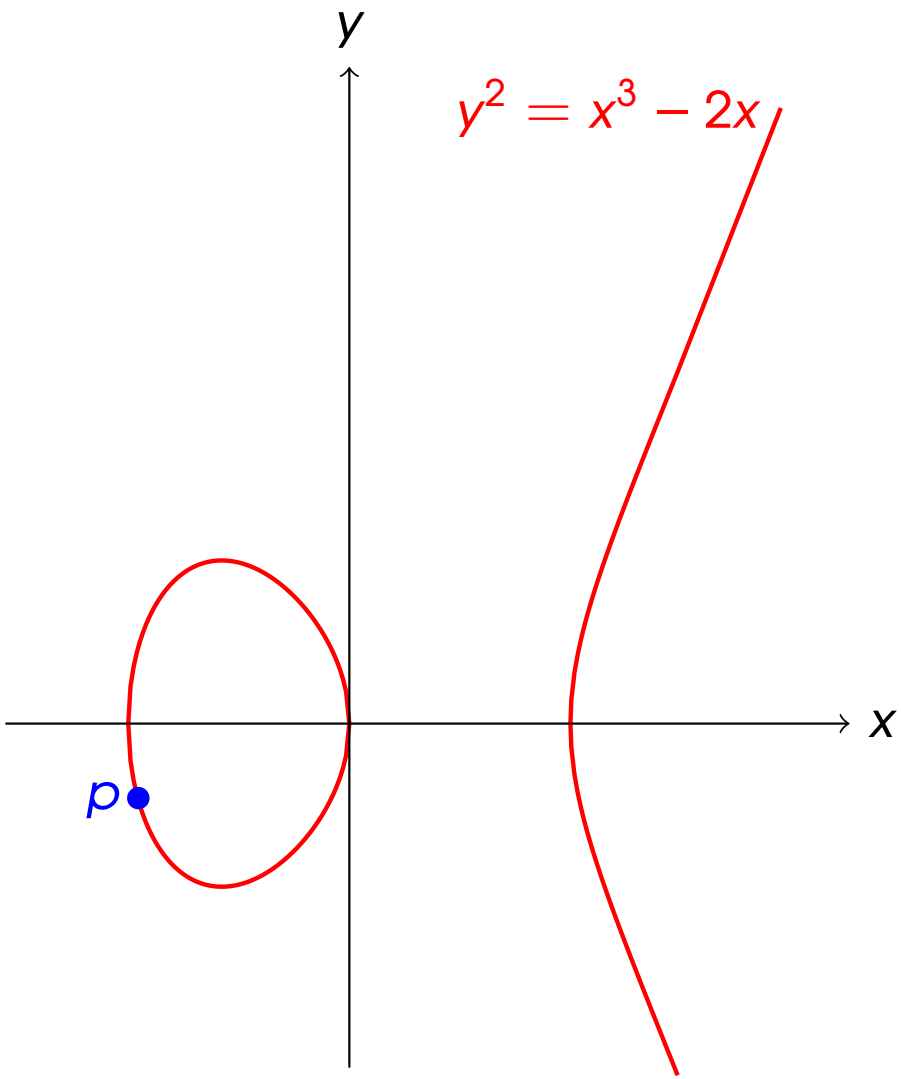
CVbum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

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

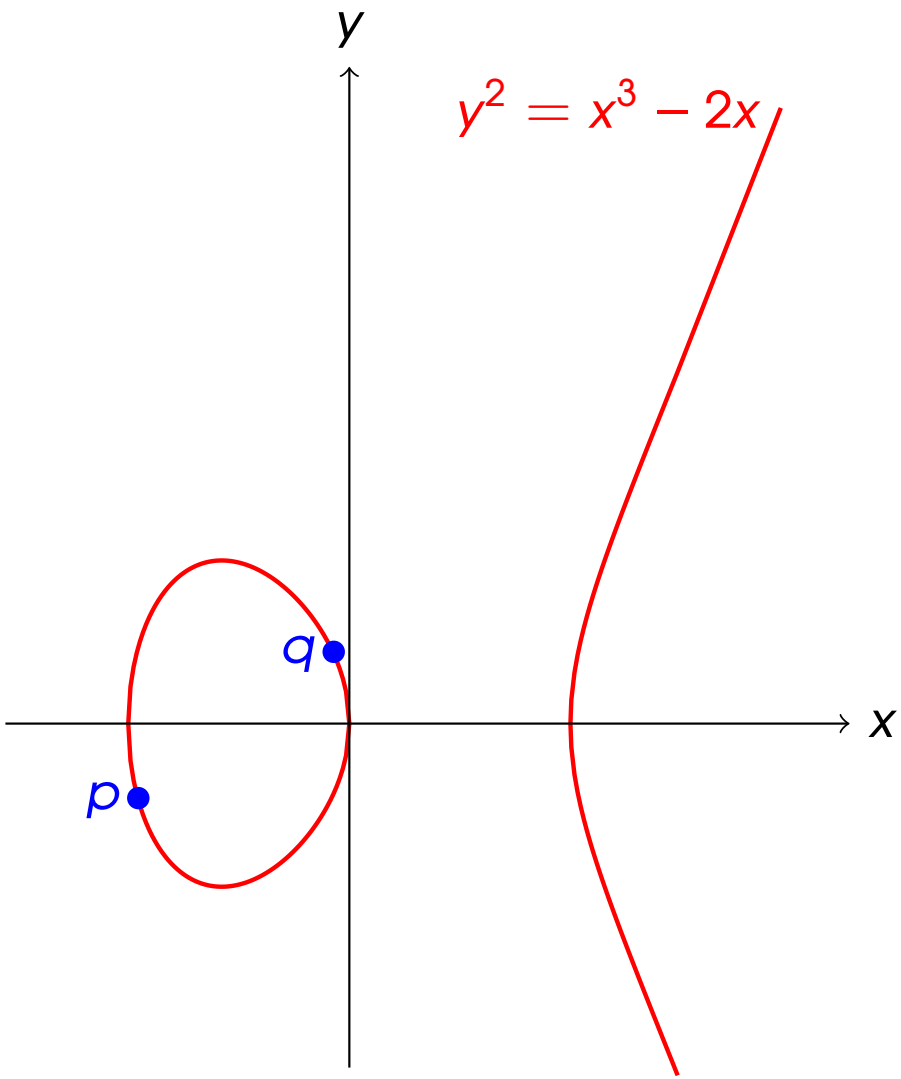
Une équation cubique



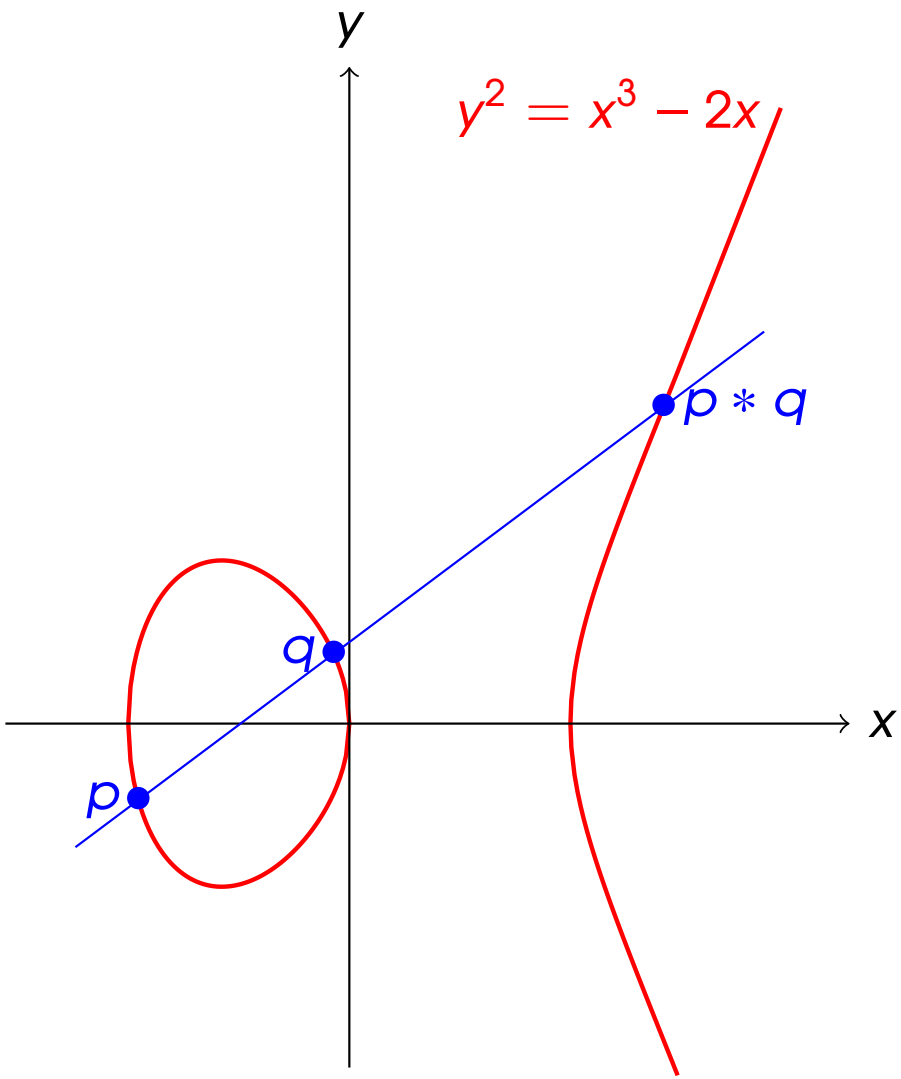
Une équation cubique



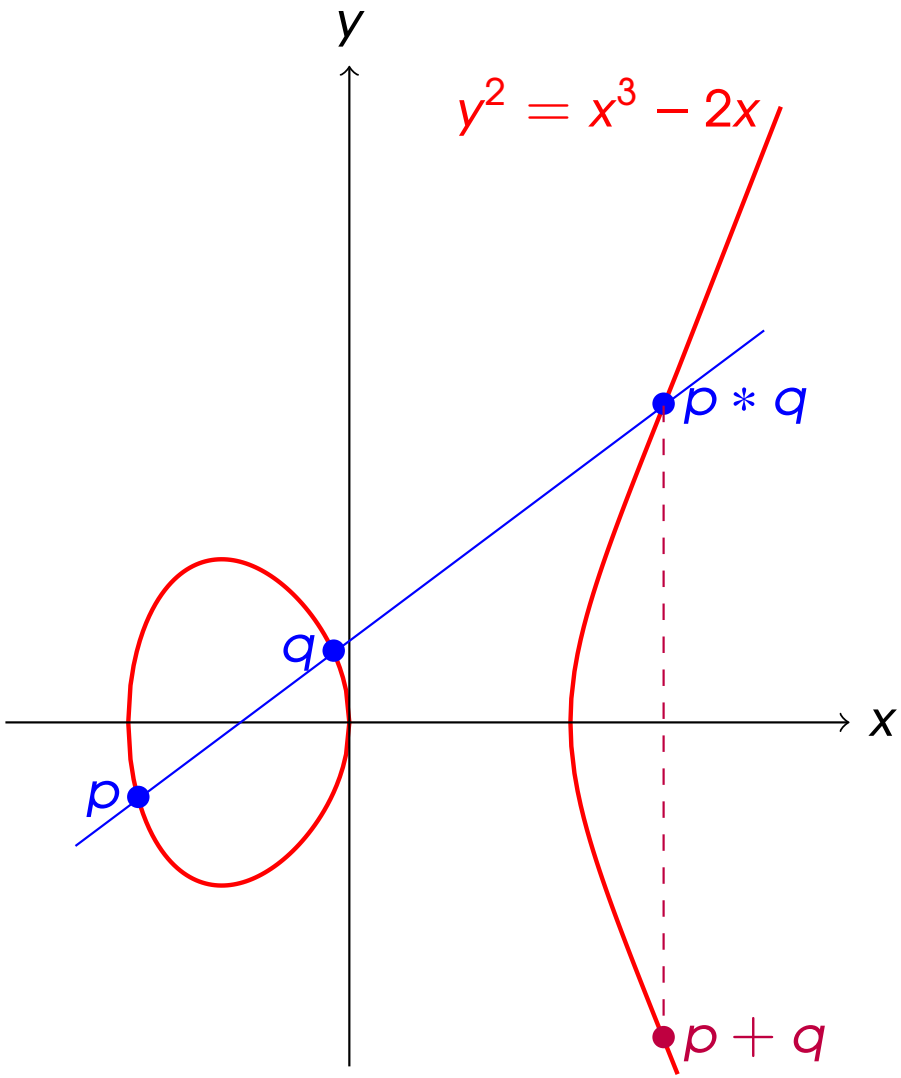
Une équation cubique



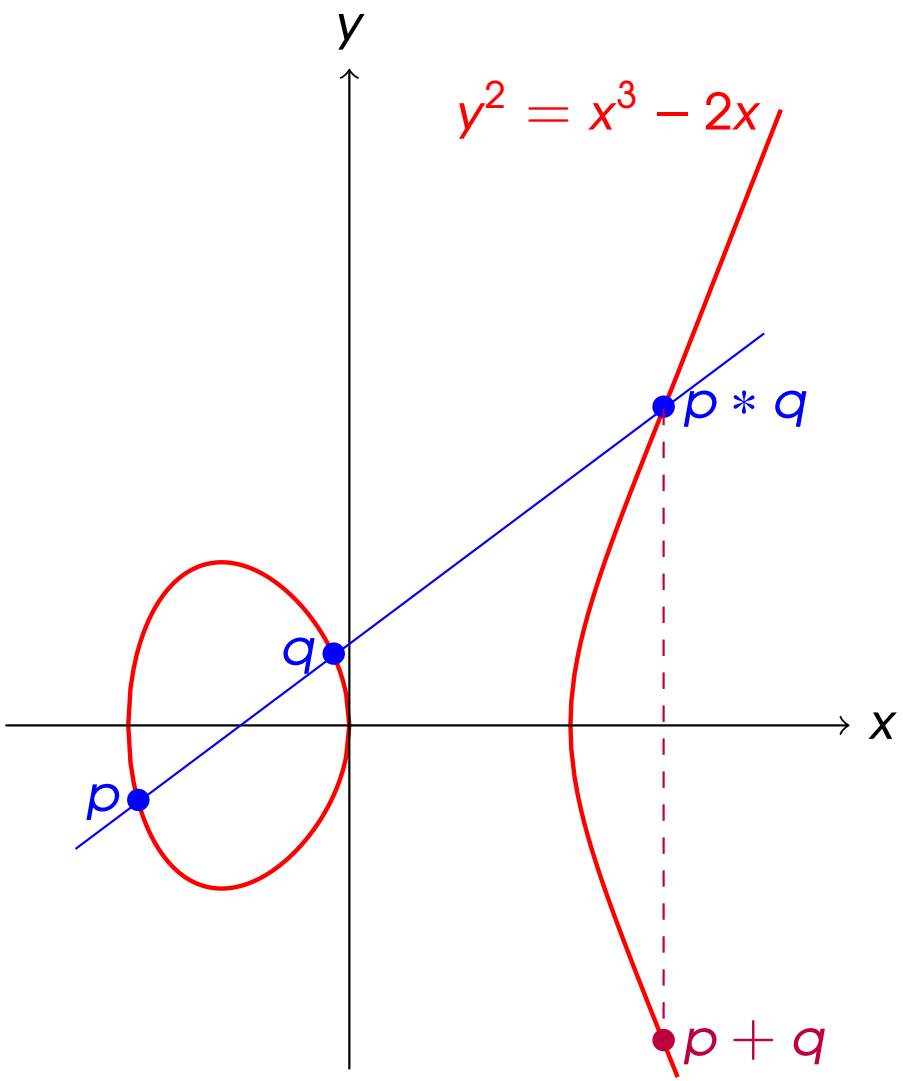
Une équation cubique



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).

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).

Conséquence de la conjecture de Lang (Caporaso, Harris, Mazur, 1997) : le nombre de solutions rationnelles d'une courbe de genre $\geqslant 2$ est uniformément majoré en fonction de son genre !

Le 10^{e} problème de Hilbert

David Hilbert, 1900, Congrès international des mathématiciens :

Le 10^{e} 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 10^{e} 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.

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 10^{e} 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 10^e 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 10^{e} 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 10^{e} 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 10^{e} 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

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

en $m + 1$ variables telle qu'aucun algorithme ne puisse dire, étant donné un entier $a \in \mathbf{Z}$, si l'équation

$$f(a, x_1, \ldots, x_m) = 0$$

possède une solution dans $\mathbf{Z}^m$ 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 10^{e} 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

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

en $m + 1$ variables telle qu'aucun algorithme ne puisse dire, étant donné un entier $a \in \mathbf{Z}$, si l'équation

$$f(a, x_1, \ldots, x_m) = 0$$

possède une solution dans $\mathbf{Z}^m$ 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 (Masser, Oesterlé, 1985)

Pour tout $\partial > 1$*, il existe* $K_\partial > 0$ *de sorte que l'on ait :*
Si A, B, C *sont trois entiers premiers entre eux tels que* $A + B = C$*, alors*

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

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 (Masser, Oesterlé, 1985)

Pour tout $\partial > 1$, il existe $K_\partial > 0$ de sorte que l'on ait :
Si A, B, C sont trois entiers premiers entre eux tels que $A + B = C$, alors

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

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) :

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

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

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

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

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

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

d'où, si $n > 3\partial$,

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

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

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

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

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

d'où, si $n > 3\partial$,

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

Ainsi, on contrôle les solutions de l'équation de Fermat en degré $n > 3\partial$.
Si n est assez grand, elles sont nécessairement toutes triviales.

La conjecture ABC pour les polynômes

Théorème (Stothers, 1981 ; Mason, 1984)

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

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

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

La conjecture ABC pour les polynômes

Théorème (Stothers, 1981 ; Mason, 1984)

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

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

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

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

La conjecture ABC pour les polynômes

Théorème (Stothers, 1981 ; Mason, 1984)

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

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

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

Preuve : 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

Théorème (Stothers, 1981 ; Mason, 1984)

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

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

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

Preuve : 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

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

La conjecture ABC pour les polynômes

Théorème (Stothers, 1981 ; Mason, 1984)

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

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

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

Preuve : 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

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

On a donc $\deg(C) \leqslant v(ABC) - 1$, 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 premiers entre eux $P, Q, R \in \mathbf{C}[t]$, 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 $n < 3$.

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, ∞.

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.

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.

Inversement :

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. »

Version géométrique --- immense généralisation du théorème de Stothers-Mason : Vojta, McQuillan, Yamanoi...