Comment des figures géométriques nous parlent de nombres entiers

Cyril Demarche

Université Pierre et Marie Curie (Paris 6)
Institut de Mathématiques de Jussieu

Mathematic Park, 29 novembre 2013

Rappels : nombres rationnels, nombres irrationnels

Je vais vous parler d'arithmétique. L'arithmétique, c'est l'étude des propriétés des nombres entiers et rationnels.

Rappels : nombres rationnels, nombres irrationnels

Je vais vous parler d'arithmétique. L'arithmétique, c'est l'étude des propriétés des nombres entiers et rationnels.

Un petit rappel : parmi tous les nombres réels (les nombres à virgule habituels), il y a ceux qui sont des fractions (les nombres rationnels) et ceux qui ne sont pas des fractions (les irrationnels).

Rappels : nombres rationnels, nombres irrationnels

Je vais vous parler d'arithmétique. L'arithmétique, c'est l'étude des propriétés des nombres entiers et rationnels.

Un petit rappel : parmi tous les nombres réels (les nombres à virgule habituels), il y a ceux qui sont des fractions (les nombres rationnels) et ceux qui ne sont pas des fractions (les irrationnels).

La plupart des nombres réels sont des nombres irrationnels : les fractions sont "rares" parmi tous les nombres possibles. Et les nombres entiers sont encore plus rares.

Rappels : nombres rationnels, nombres irrationnels

Je vais vous parler d'arithmétique. L'arithmétique, c'est l'étude des propriétés des nombres entiers et rationnels.

Un petit rappel : parmi tous les nombres réels (les nombres à virgule habituels), il y a ceux qui sont des fractions (les nombres rationnels) et ceux qui ne sont pas des fractions (les irrationnels).

La plupart des nombres réels sont des nombres irrationnels : les fractions sont "rares" parmi tous les nombres possibles. Et les nombres entiers sont encore plus rares.

Par exemple, des nombres comme $\sqrt{2} = 1.414\ldots$, $\sqrt{3} = 1.732\ldots$, $\pi = 3.14159\ldots$ ou $0.12345678910111213141516\ldots$ sont des nombres irrationnels.

Rappels : nombres rationnels, nombres irrationnels

Je vais vous parler d'arithmétique. L'arithmétique, c'est l'étude des propriétés des nombres entiers et rationnels.

Un petit rappel : parmi tous les nombres réels (les nombres à virgule habituels), il y a ceux qui sont des fractions (les nombres rationnels) et ceux qui ne sont pas des fractions (les irrationnels).

La plupart des nombres réels sont des nombres irrationnels : les fractions sont "rares" parmi tous les nombres possibles. Et les nombres entiers sont encore plus rares.

Par exemple, des nombres comme $\sqrt{2} = 1.414\ldots$, $\sqrt{3} = 1.732\ldots$, $\pi = 3.14159\ldots$ ou $0.12345678910111213141516\ldots$ sont des nombres irrationnels.

En revanche, les nombres 1, 42, $0.33333\ldots$, 0.5, $1.232323\ldots$ sont des nombres rationnels.

Rappels : nombres rationnels, nombres irrationnels

Je vais vous parler d'arithmétique. L'arithmétique, c'est l'étude des propriétés des nombres entiers et rationnels.

Un petit rappel : parmi tous les nombres réels (les nombres à virgule habituels), il y a ceux qui sont des fractions (les nombres rationnels) et ceux qui ne sont pas des fractions (les irrationnels).

La plupart des nombres réels sont des nombres irrationnels : les fractions sont "rares" parmi tous les nombres possibles. Et les nombres entiers sont encore plus rares.

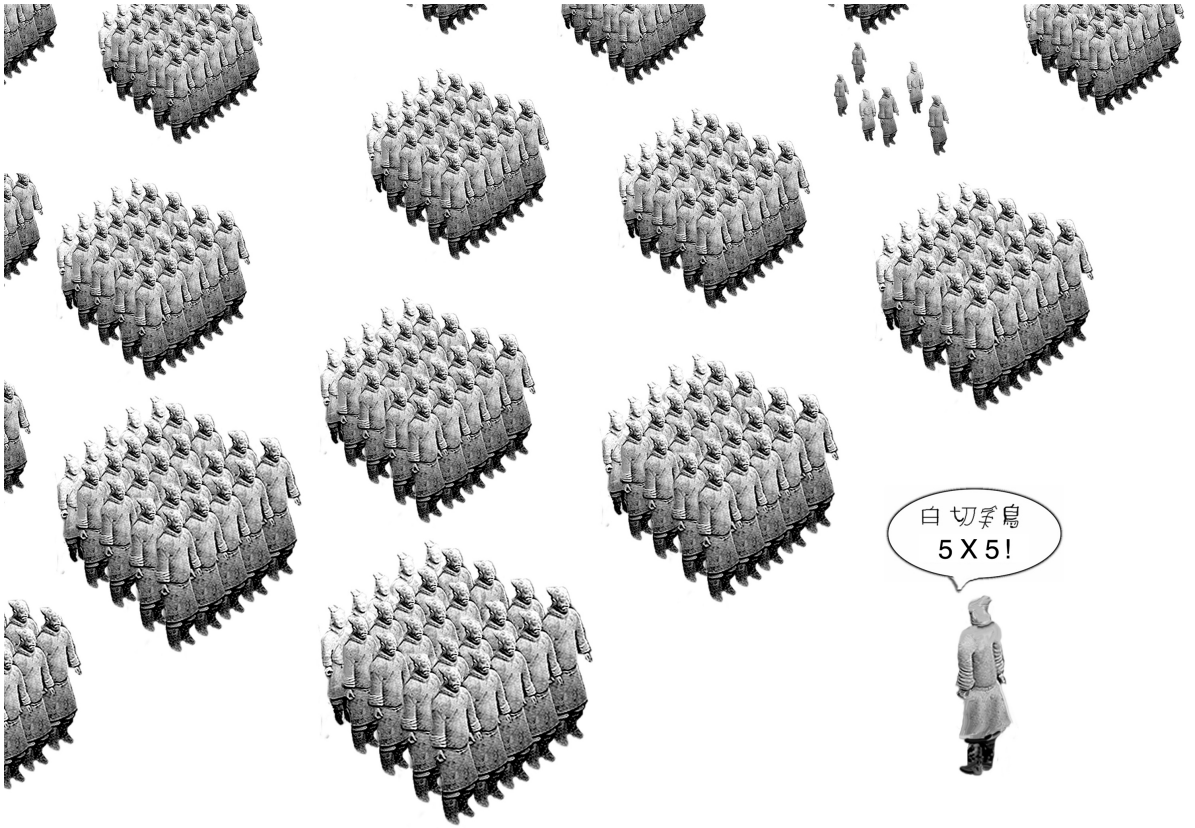
Par exemple, des nombres comme $\sqrt{2} = 1.414\ldots$, $\sqrt{3} = 1.732\ldots$, $\pi = 3.14159\ldots$ ou $0.12345678910111213141516\ldots$ sont des nombres irrationnels.

En revanche, les nombres 1, 42, $0.33333\ldots$, 0.5, $1.232323\ldots$ sont des nombres rationnels.

Dans tout l'exposé, on travaillera avec les nombres entiers ou rationnels, et pas avec les nombres irrationnels.

Deux premiers exemples simples

Le problème suivant a été étudié dès la Chine antique (III ème siècle après JC) :



$N \equiv 6 \pmod{25}$

Deux premiers exemples simples

Questions

1. *Un général veut compter les soldats de son armée.*

Deux premiers exemples simples

Questions

1. *Un général veut compter les soldats de son armée.*
   Il demande aux soldats de se grouper par trois, et il constate qu'il reste deux soldats tout seuls à la fin.

Deux premiers exemples simples

Questions

1. *Un général veut compter les soldats de son armée.*
   Il demande aux soldats de se grouper par trois, et il constate qu'il reste deux soldats tout seuls à la fin.
   Puis il leur demande de se grouper par cinq, et il en reste trois.

Deux premiers exemples simples

Questions

1. *Un général veut compter les soldats de son armée.*
   Il demande aux soldats de se grouper par trois, et il constate qu'il reste deux soldats tout seuls à la fin.
   Puis il leur demande de se grouper par cinq, et il en reste trois.
   Enfin, il leur demande de se grouper par sept, et il en reste deux.

Deux premiers exemples simples

Questions

1. *Un général veut compter les soldats de son armée.*
   Il demande aux soldats de se grouper par trois, et il constate qu'il reste deux soldats tout seuls à la fin.
   Puis il leur demande de se grouper par cinq, et il en reste trois.
   Enfin, il leur demande de se grouper par sept, et il en reste deux.
   Combien y a-t-il de soldats au total ?

Deux premiers exemples simples

Questions

1. *Un général veut compter les soldats de son armée.*
   Il demande aux soldats de se grouper par trois, et il constate qu'il reste deux soldats tout seuls à la fin.
   Puis il leur demande de se grouper par cinq, et il en reste trois.
   Enfin, il leur demande de se grouper par sept, et il en reste deux.
   Combien y a-t-il de soldats au total ?
2. *Une variante : dans un pays lointain appelé la Ecnarf, on utilise une monnaie (le orue) et la banque nationale ne fournit que des pièces de 5 et de 7 orues. Un habitant souhaite acheter une baguette de pain pour 1 orue.*

Deux premiers exemples simples

Questions

1. *Un général veut compter les soldats de son armée.*
   Il demande aux soldats de se grouper par trois, et il constate qu'il reste deux soldats tout seuls à la fin.
   Puis il leur demande de se grouper par cinq, et il en reste trois.
   Enfin, il leur demande de se grouper par sept, et il en reste deux.
   Combien y a-t-il de soldats au total ?
2. *Une variante : dans un pays lointain appelé la Ecnarf, on utilise une monnaie (le orue) et la banque nationale ne fournit que des pièces de 5 et de 7 orues. Un habitant souhaite acheter une baguette de pain pour 1 orue.*
   Comment fait-il ?

Deux premiers exemples simples

Questions

1. *Un général veut compter les soldats de son armée.*
   Il demande aux soldats de se grouper par trois, et il constate qu'il reste deux soldats tout seuls à la fin.
   Puis il leur demande de se grouper par cinq, et il en reste trois.
   Enfin, il leur demande de se grouper par sept, et il en reste deux.
   Combien y a-t-il de soldats au total ?
2. *Une variante : dans un pays lointain appelé la Ecnarf, on utilise une monnaie (le orue) et la banque nationale ne fournit que des pièces de 5 et de 7 orues. Un habitant souhaite acheter une baguette de pain pour 1 orue.*
   Comment fait-il ?
   Plus généralement, quelles sommes peut-on payer avec cette monnaie ? Et si on remplaçait toutes les pièces de 5 et 7 orues par des pièces de 6 et 9 orues ?

Reformulation

On peut reformuler ces problèmes par les équations suivantes :

Reformulation

On peut reformuler ces problèmes par les équations suivantes :

1. *Si on note n le nombre de soldats, on cherche des nombres entiers positifs n, x, y, z tels que*

$$\begin{cases} n = 3x + 2 \\ n = 5y + 3 \\ n = 7z + 2 \end{cases}.$$

Reformulation

On peut reformuler ces problèmes par les équations suivantes :

1. *Si on note n le nombre de soldats, on cherche des nombres entiers positifs n, x, y, z tels que*

$$\begin{cases} n = 3x + 2 \\ n = 5y + 3 \\ n = 7z + 2 \end{cases}.$$

2. *On cherche des entiers relatifs x, y tels que*

$$5x + 7y = 1\,.$$

Dans le cas général, étant donné un entier n, on cherche des entiers relatifs x, y tels que

$$5x + 7y = n\,.$$

Solution du problème des soldats

$$\begin{cases} n = 3x + 2 \\ n = 5y + 3 \\ n = 7z + 2 \end{cases}.$$

Solution du problème des soldats

$$\begin{cases} n = 3x + 2 \\ n = 5y + 3 \\ n = 7z + 2 \end{cases}.$$

Pour la première équation, il est clair que les solutions sont les entiers qui sont "multiples de trois plus deux", donc les entiers $2, 5, 8, \ldots$.

Solution du problème des soldats

$$\begin{cases} n = 3x + 2 \\ n = 5y + 3 \\ n = 7z + 2 \end{cases}.$$

Pour la première équation, il est clair que les solutions sont les entiers qui sont "multiples de trois plus deux", donc les entiers $2, 5, 8, \ldots$.

Si on considère les deux premières conditions, on remarque que $n = 8$ est solution. Et si un entier n vérifie ces deux conditions, alors l'entier $n + 15$ les vérifie également $(15 = 3.5)$.

Solution du problème des soldats

$$\begin{cases} n = 3x + 2 \\ n = 5y + 3 \\ n = 7z + 2 \end{cases}.$$

Pour la première équation, il est clair que les solutions sont les entiers qui sont "multiples de trois plus deux", donc les entiers $2, 5, 8, \ldots$.

Si on considère les deux premières conditions, on remarque que $n = 8$ est solution. Et si un entier n vérifie ces deux conditions, alors l'entier $n + 15$ les vérifie également $(15 = 3.5)$.

Donc les solutions des deux premières équations sont de la forme "8 plus un multiple de 15", donc de la forme $n = 8 + 15.k$ (k entier positif quelconque), donc dans la liste $8, 23, 38, \ldots$.

Solution du problème des soldats

$$\begin{cases} n = 3x + 2 \\ n = 5y + 3 \\ n = 7z + 2 \end{cases}.$$

Solution du problème des soldats

$$\begin{cases} n = 3x + 2 \\ n = 5y + 3 \\ n = 7z + 2 \end{cases}.$$

Si on considère les trois conditions, on voit que 23 est solution du problème, et que si un entier n est solution, alors l'entier $n + 105$ l'est également ($105 = 3.5.7$).

Solution du problème des soldats

$$\begin{cases} n = 3x + 2 \\ n = 5y + 3 \\ n = 7z + 2 \end{cases}.$$

Si on considère les trois conditions, on voit que 23 est solution du problème, et que si un entier n est solution, alors l'entier $n + 105$ l'est également ($105 = 3.5.7$).

Donc le nombre n est de la forme "23 plus un multiple de 105", donc de la forme $n = 23 + 105.k$ (k entier positif quelconque), donc dans la liste $23, 128, 233, 338, 443, \ldots$.

Solution du problème des soldats

$$\begin{cases} n = 3x + 2 \\ n = 5y + 3 \\ n = 7z + 2 \end{cases}.$$

Si on considère les trois conditions, on voit que 23 est solution du problème, et que si un entier n est solution, alors l'entier $n + 105$ l'est également ($105 = 3.5.7$).

Donc le nombre n est de la forme "23 plus un multiple de 105", donc de la forme $n = 23 + 105.k$ (k entier positif quelconque), donc dans la liste $23, 128, 233, 338, 443, \ldots$.

Il y a donc une infinité de solutions. La plus petite solution est $n = 23$. Si le général sait que son armée compte entre 400 et 500 soldats, alors il peut conclure que le nombre de soldats est exactement 443.

Solution du problème des pièces de monnaie

$$5x + 7y = 1\,.$$

Solution du problème des pièces de monnaie

$$5x + 7y = 1\,.$$

- Pour le problème initial des pièces de monnaie, on trouve facilement la formule suivante :

$$3.7 - 4.5 = 1\,.$$

Solution du problème des pièces de monnaie

$$5x + 7y = 1\,.$$

- Pour le problème initial des pièces de monnaie, on trouve facilement la formule suivante :

$$3.7 - 4.5 = 1\,.$$

Notre personnage peut payer un orue en donnant trois pièces de 7 orues et le commerçant lui rendra quatre pièces de 5 orues.

Solution du problème des pièces de monnaie

$$5x + 7y = 1\,.$$

- Pour le problème initial des pièces de monnaie, on trouve facilement la formule suivante :

$$3.7 - 4.5 = 1\,.$$

Notre personnage peut payer un orue en donnant trois pièces de 7 orues et le commerçant lui rendra quatre pièces de 5 orues.
Pour payer 10 orues, il suffit de tout multiplier par 10 :

$$30.7 - 40.5 = 10\,.$$

Solution du problème des pièces de monnaie

$$5x + 7y = 1\,.$$

- Pour le problème initial des pièces de monnaie, on trouve facilement la formule suivante :

$$3.7 - 4.5 = 1\,.$$

Notre personnage peut payer un orue en donnant trois pièces de 7 orues et le commerçant lui rendra quatre pièces de 5 orues.
Pour payer 10 orues, il suffit de tout multiplier par 10 :

$$30.7 - 40.5 = 10\,.$$

De cette façon, on peut payer toutes les sommes (entières) possibles.

Solution du problème des pièces de monnaie

$$5x + 7y = 1\,.$$

- Pour le problème initial des pièces de monnaie, on trouve facilement la formule suivante :

$$3.7 - 4.5 = 1\,.$$

Notre personnage peut payer un orue en donnant trois pièces de 7 orues et le commerçant lui rendra quatre pièces de 5 orues.
Pour payer 10 orues, il suffit de tout multiplier par 10 :

$$30.7 - 40.5 = 10\,.$$

De cette façon, on peut payer toutes les sommes (entières) possibles.

- Avec des pièces de 6 et 9 orue, on remarque que l'on ne peut obtenir que des multiples de 3 en combinant 6 et 9 orues. Donc on ne pourra pas payer la somme de 1 orue. Le problème n'a pas de solution.

Et la géométrie dans tout ça ?

On peut interpréter les problèmes précédents de manière géométrique.

Et la géométrie dans tout ça ?

On peut interpréter les problèmes précédents de manière géométrique.

Commençons par le second problème : vous savez que l'équation $5.x + 7.y = 1$ est une équation de droite. On note Δ cette droite.

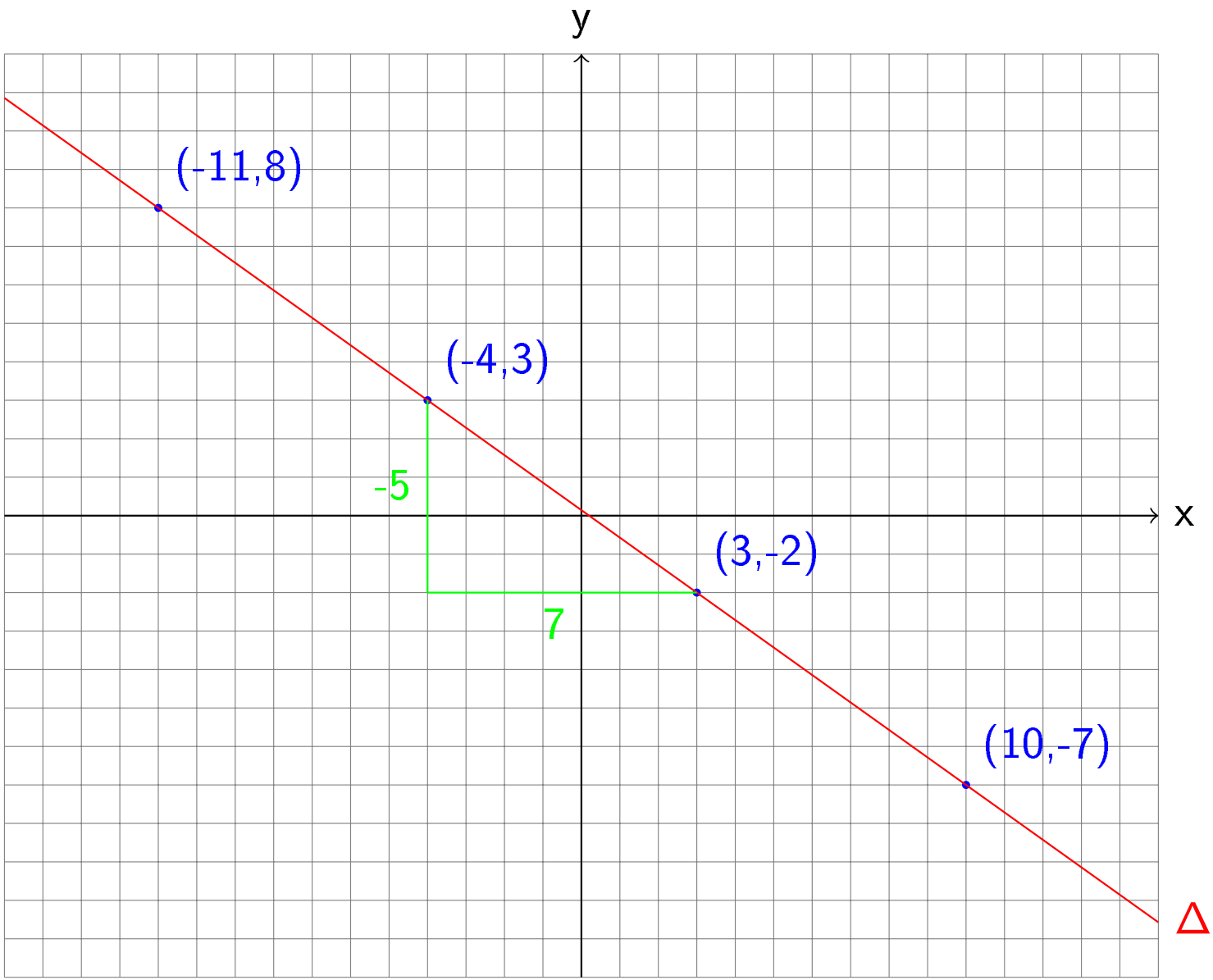
Et la géométrie dans tout ça ?

On peut interpréter les problèmes précédents de manière géométrique.

Commençons par le second problème : vous savez que l'équation $5.x + 7.y = 1$ est une équation de droite. On note Δ cette droite.

Le problème des pièces se traduit géométriquement en cherchant les points de la droite Δ qui ont des coordonnées entières. On voit alors sur la figure suivante les solutions à notre problème.

Géométrie pour le problème des pièces



$\Delta : 5x + 7y = 1$

Géométrie pour le problème des soldats

De même, pour le problème des soldats, on se rend compte que les trois équations correspondent aussi à une droite, non pas dans le plan, mais dans un espace de dimension plus grande (dimension 4...).

Géométrie pour le problème des soldats

De même, pour le problème des soldats, on se rend compte que les trois équations correspondent aussi à une droite, non pas dans le plan, mais dans un espace de dimension plus grande (dimension 4...).

Donc finalement, quand on a résolu ces problèmes, on a en fait recherché les points à coordonnés entières sur une droite.

Géométrie pour le problème des soldats

De même, pour le problème des soldats, on se rend compte que les trois équations correspondent aussi à une droite, non pas dans le plan, mais dans un espace de dimension plus grande (dimension 4...).

Donc finalement, quand on a résolu ces problèmes, on a en fait recherché les points à coordonnés entières sur une droite.

Dans ces questions, l'interprétation géométrique ne simplifie pas vraiment le problème : on a réussi à résoudre l'équation sans passer par la géométrie.

Géométrie pour le problème des soldats

De même, pour le problème des soldats, on se rend compte que les trois équations correspondent aussi à une droite, non pas dans le plan, mais dans un espace de dimension plus grande (dimension 4...).

Donc finalement, quand on a résolu ces problèmes, on a en fait recherché les points à coordonnés entières sur une droite.

Dans ces questions, l'interprétation géométrique ne simplifie pas vraiment le problème : on a réussi à résoudre l'équation sans passer par la géométrie.

Dans la suite, on va considérer des problèmes d'arithmétique plus complexes, où la géométrie sera vraiment nécessaire pour les résoudre.

Géométrie pour le problème des soldats

De même, pour le problème des soldats, on se rend compte que les trois équations correspondent aussi à une droite, non pas dans le plan, mais dans un espace de dimension plus grande (dimension 4...).

Donc finalement, quand on a résolu ces problèmes, on a en fait recherché les points à coordonnés entières sur une droite.

Dans ces questions, l'interprétation géométrique ne simplifie pas vraiment le problème : on a réussi à résoudre l'équation sans passer par la géométrie.

Dans la suite, on va considérer des problèmes d'arithmétique plus complexes, où la géométrie sera vraiment nécessaire pour les résoudre.

Les problèmes considérés jusqu'ici étaient relativement faciles parce que c'était des problèmes qui concernaient des droites, et la géométrie des droites est très simple.

Bilan

On peut donc résumer les problèmes précédents en disant que :

Bilan

On peut donc résumer les problèmes précédents en disant que :

les problèmes d'arithmétique de degré 1 sont assez faciles à résoudre.

Bilan

On peut donc résumer les problèmes précédents en disant que :

les problèmes d'arithmétique de degré 1 sont assez faciles à résoudre.

Sauf erreur, c'est au programme de Terminale S, spécialité Math.

Un nouvel exemple

Restons à l'antiquité, et poursuivons par un petit problème grec :

Un nouvel exemple

Restons à l'antiquité, et poursuivons par un petit problème grec :

Question

Trouver tous les nombres entiers x, y, z qui vérifient

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

Un nouvel exemple

Restons à l'antiquité, et poursuivons par un petit problème grec :

Question

Trouver tous les nombres entiers x, y, z qui vérifient

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

Par le théorème de Pythagore, cela revient à déterminer tous les triangles rectangles dont les trois côtés ont des longueurs entières.

Un nouvel exemple

Restons à l'antiquité, et poursuivons par un petit problème grec :

Question

Trouver tous les nombres entiers x, y, z qui vérifient

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

Par le théorème de Pythagore, cela revient à déterminer tous les triangles rectangles dont les trois côtés ont des longueurs entières.

Un nouvel exemple

Restons à l'antiquité, et poursuivons par un petit problème grec :

Question

Trouver tous les nombres entiers x, y, z qui vérifient

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

Par le théorème de Pythagore, cela revient à déterminer tous les triangles rectangles dont les trois côtés ont des longueurs entières.

Question

Pouvez-vous trouver des solutions ?

Exemples de solutions

On vérifie que

$$3^2 + 4^2 = 5^2 \,,$$

Exemples de solutions

On vérifie que

$$3^2 + 4^2 = 5^2\,,$$

et aussi

$$6^2 + 8^2 = 10^2\,,$$

$$9^2 + 12^2 = 15^2\,,$$

Exemples de solutions

On vérifie que

$$3^2 + 4^2 = 5^2\,,$$

et aussi

$$6^2 + 8^2 = 10^2\,,$$

$$9^2 + 12^2 = 15^2\,,$$

et on peut trouver une infinité de solutions de cette façon à partir de la première, en multipliant les nombres $3, 4, 5$ par n'importe quel entier.

Exemples de solutions

On vérifie que

$$3^2 + 4^2 = 5^2 \,,$$

et aussi

$$6^2 + 8^2 = 10^2 \,,$$

$$9^2 + 12^2 = 15^2 \,,$$

et on peut trouver une infinité de solutions de cette façon à partir de la première, en multipliant les nombres $3, 4, 5$ par n'importe quel entier. Par exemple, en multipliant par 16, on trouve

$$48^2 + 64^2 = 80^2 \,.$$

Exemples de solutions

On vérifie que

$$3^2 + 4^2 = 5^2 \,,$$

et aussi

$$6^2 + 8^2 = 10^2 \,,$$

$$9^2 + 12^2 = 15^2 \,,$$

et on peut trouver une infinité de solutions de cette façon à partir de la première, en multipliant les nombres $3, 4, 5$ par n'importe quel entier. Par exemple, en multipliant par 16, on trouve

$$48^2 + 64^2 = 80^2 \,.$$

Mais toutes ces solutions sont un peu les mêmes : on peut les simplifier et on retrouve la première.

Autres solutions

Pouvez-vous trouver d'autres solutions, vraiment différentes ?

Autres solutions

Pouvez-vous trouver d'autres solutions, vraiment différentes ?

Deux autres solutions :

$$5^2 + 12^2 = 13^2\,,$$
$$8^2 + 15^2 = 17^2\,.$$

Toutes les solutions de $x^2 + y^2 = z^2$?

Ces exemples de solutions ne suffisent pas.

Toutes les solutions de $x^2 + y^2 = z^2$?

Ces exemples de solutions ne suffisent pas.

Comment déterminer TOUTES les solutions du problème ?

Toutes les solutions de $x^2 + y^2 = z^2$?

Ces exemples de solutions ne suffisent pas.

Comment déterminer TOUTES les solutions du problème ?

Ici, la géométrie va vraiment nous être utile.

Toutes les solutions de $x^2 + y^2 = z^2$?

Ces exemples de solutions ne suffisent pas.

Comment déterminer TOUTES les solutions du problème ?

Ici, la géométrie va vraiment nous être utile.

Pour commencer, on remarque que si je pose $X = \frac{x}{z}$ et $Y = \frac{y}{z}$, le problème initial revient à trouver toutes les solutions X et Y en nombres rationnels (fractions) de l'équation

$$X^2 + Y^2 = 1\,.$$

Toutes les solutions de $x^2 + y^2 = z^2$?

Ces exemples de solutions ne suffisent pas.

Comment déterminer TOUTES les solutions du problème ?

Ici, la géométrie va vraiment nous être utile.

Pour commencer, on remarque que si je pose $X = \frac{x}{z}$ et $Y = \frac{y}{z}$, le problème initial revient à trouver toutes les solutions X et Y en nombres rationnels (fractions) de l'équation

$$X^2 + Y^2 = 1\,.$$

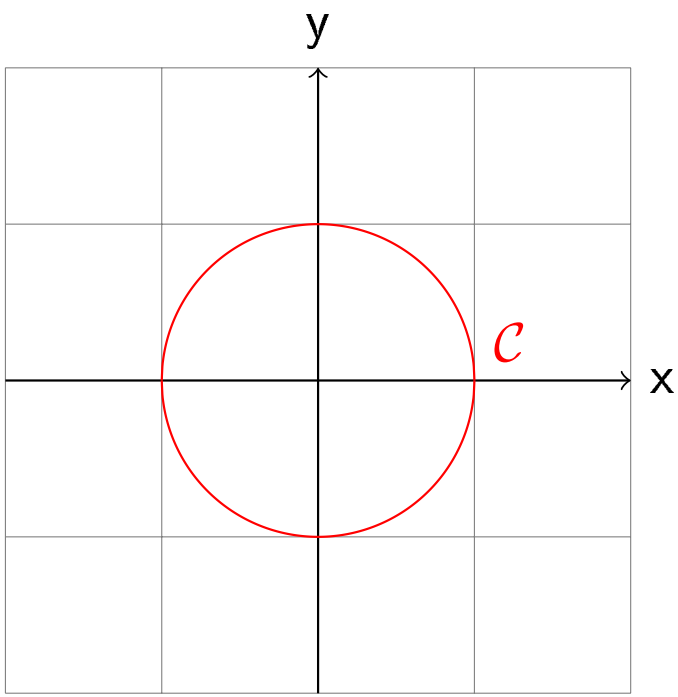
Géométriquement, que représente cette équation ?

Géométrie du problème de Pythagore

L'équation $X^2 + Y^2 = 1$ est représentée par un CERCLE : le cercle $\mathcal{C}$ de centre l'origine et de rayon 1.

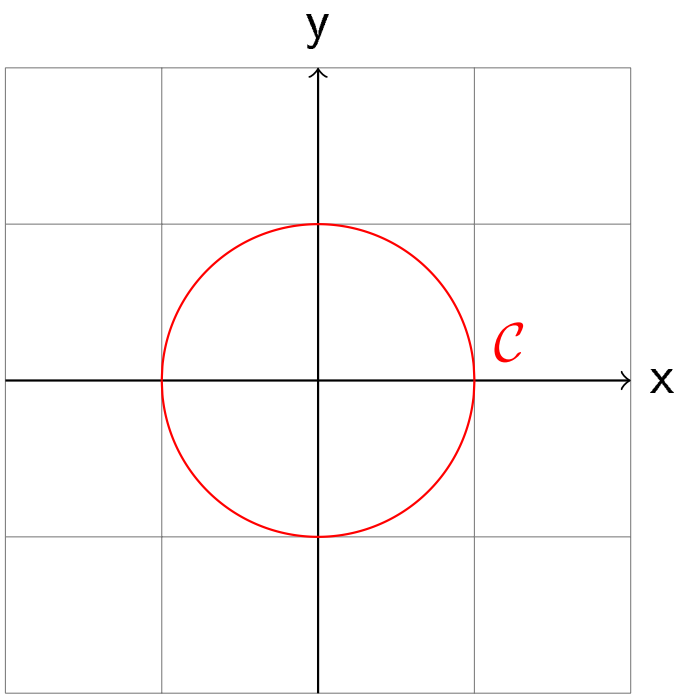
Géométrie du problème de Pythagore

L'équation $X^2 + Y^2 = 1$ est représentée par un CERCLE : le cercle $\mathcal{C}$ de centre l'origine et de rayon 1.



Géométrie du problème de Pythagore

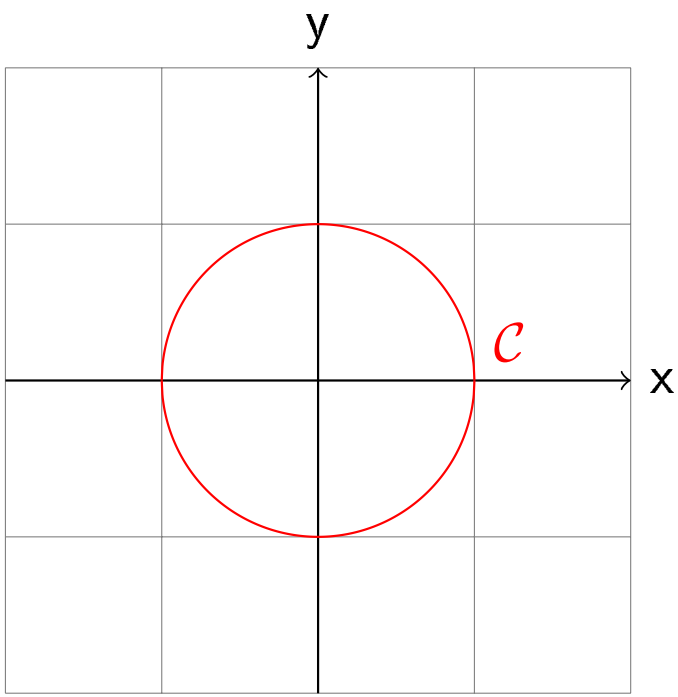
L'équation $X^2 + Y^2 = 1$ est représentée par un CERCLE : le cercle $\mathcal{C}$ de centre l'origine et de rayon 1.



En langage géométrique, le problème de Pythagore se reformule ainsi : trouver tous les points à coordonnés rationnelles sur le cercle $\mathcal{C}$.

Géométrie du problème de Pythagore

L'équation $X^2 + Y^2 = 1$ est représentée par un CERCLE : le cercle $\mathcal{C}$ de centre l'origine et de rayon 1.



En langage géométrique, le problème de Pythagore se reformule ainsi : trouver tous les points à coordonnés rationnelles sur le cercle $\mathcal{C}$.

A-t-on vraiment simplifié le problème ? ?

Un peu de géométrie

La réponse est OUI.

Un peu de géométrie

La réponse est OUI.

En effet, géométriquement, un cercle c'est PRESQUE une droite.

Un peu de géométrie

La réponse est OUI.

En effet, géométriquement, un cercle c'est PRESQUE une droite.

Et trouver les points à coordonnées rationnelles sur une droite, c'est facile.

Un peu de géométrie

La réponse est OUI.

En effet, géométriquement, un cercle c'est PRESQUE une droite.

Et trouver les points à coordonnées rationnelles sur une droite, c'est facile.

Pourquoi peut-on dire que "un cercle c'est PRESQUE une droite" ?

Un peu de géométrie

La réponse est OUI.

En effet, géométriquement, un cercle c'est PRESQUE une droite.

Et trouver les points à coordonnées rationnelles sur une droite, c'est facile.

Pourquoi peut-on dire que "un cercle c'est PRESQUE une droite" ?

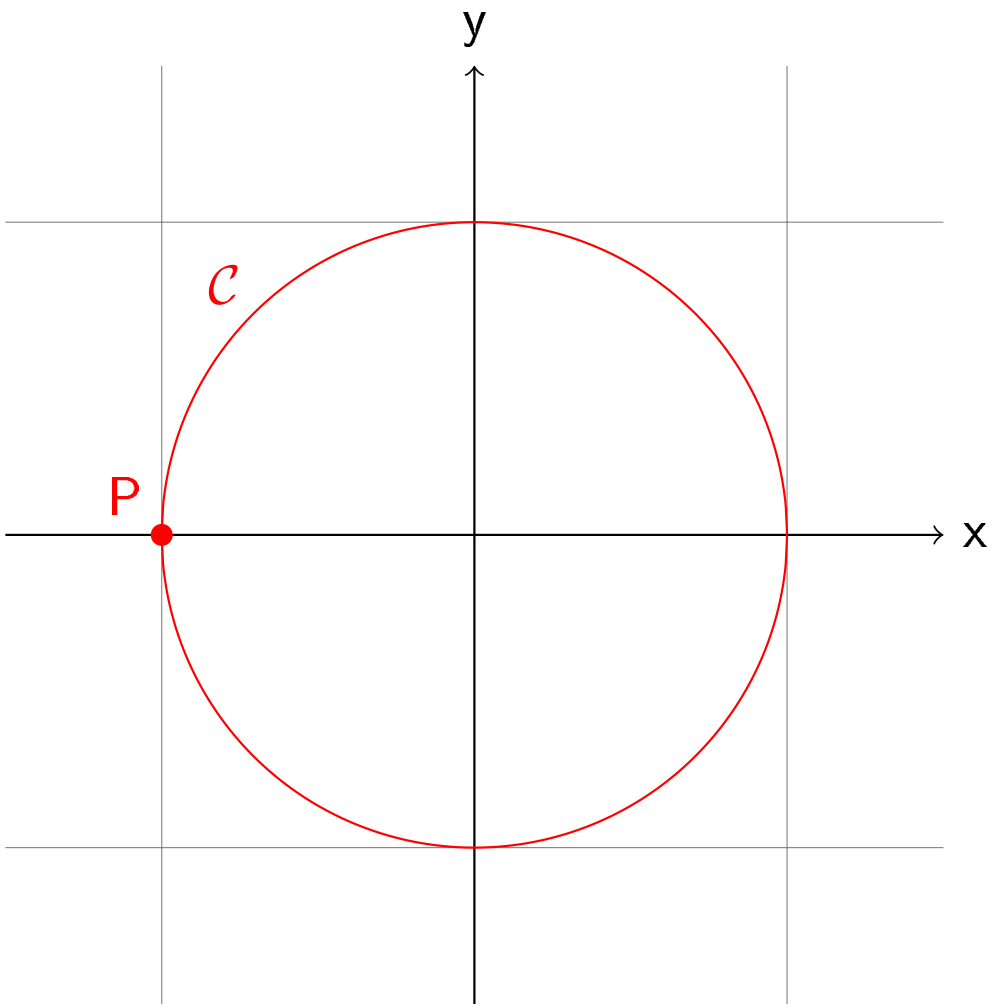
Si on enlève un point d'un cercle, on peut déplier ce cercle pour obtenir une droite (ou un segment). On va maintenant détailler cette idée.

Projection stéréographique

Considérons le cercle $\mathcal{C}$ de centre l'origine et de rayon 1. Voici la figure :

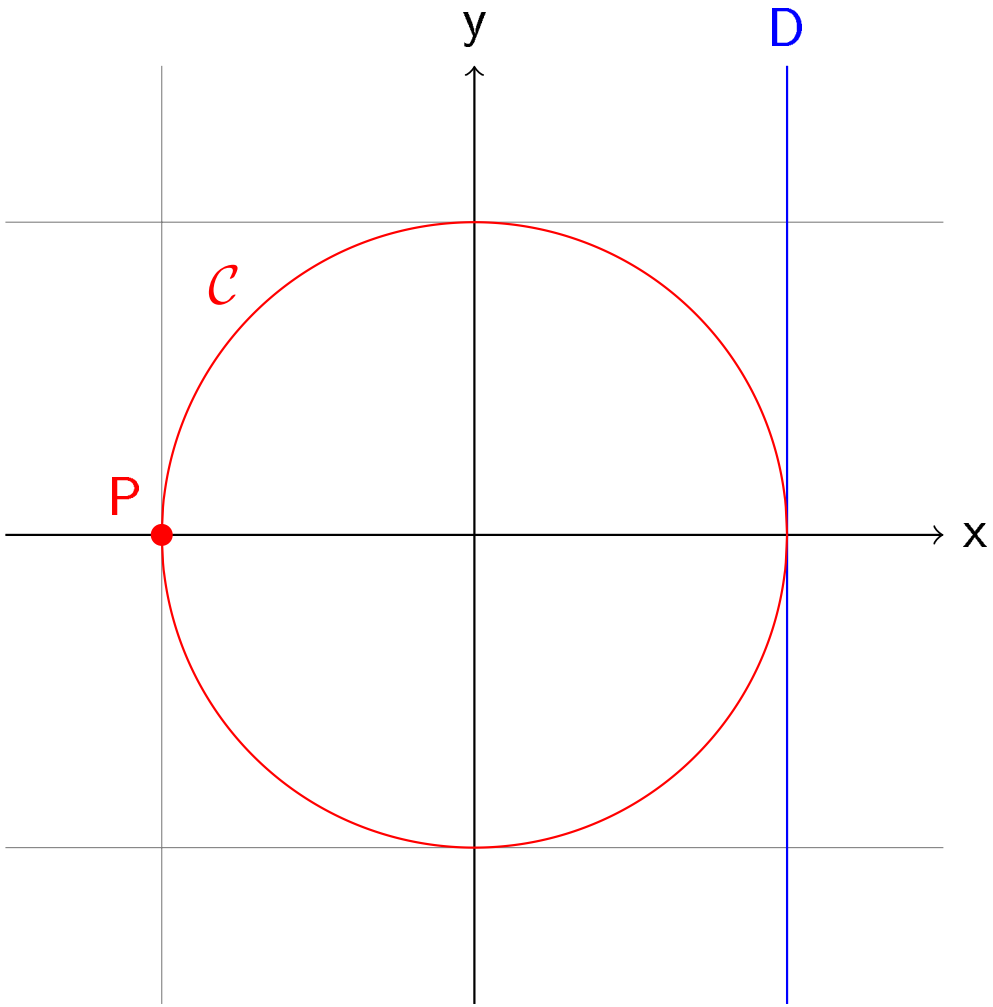
Projection stéréographique

Considérons le cercle $\mathcal{C}$ de centre l'origine et de rayon 1. Voici la figure :



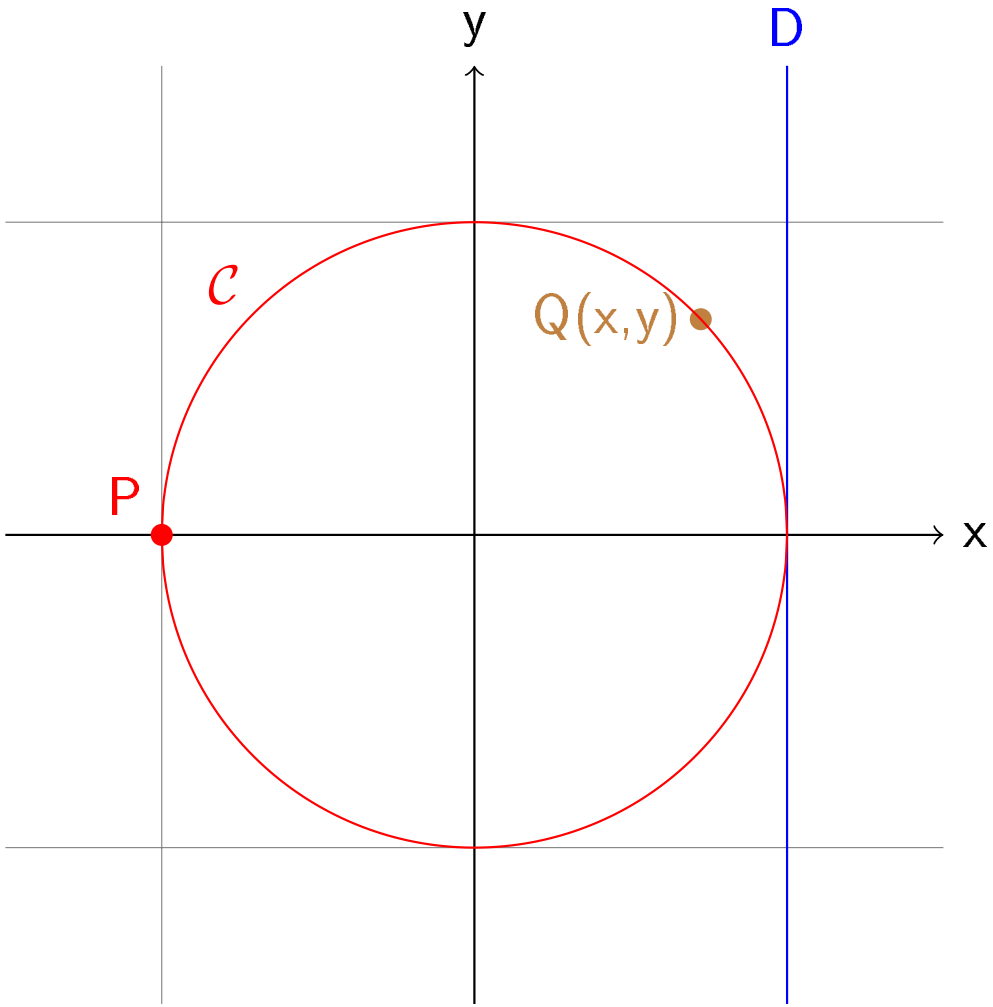
Projection stéréographique

Considérons le cercle $\mathcal{C}$ de centre l'origine et de rayon 1. Voici la figure :



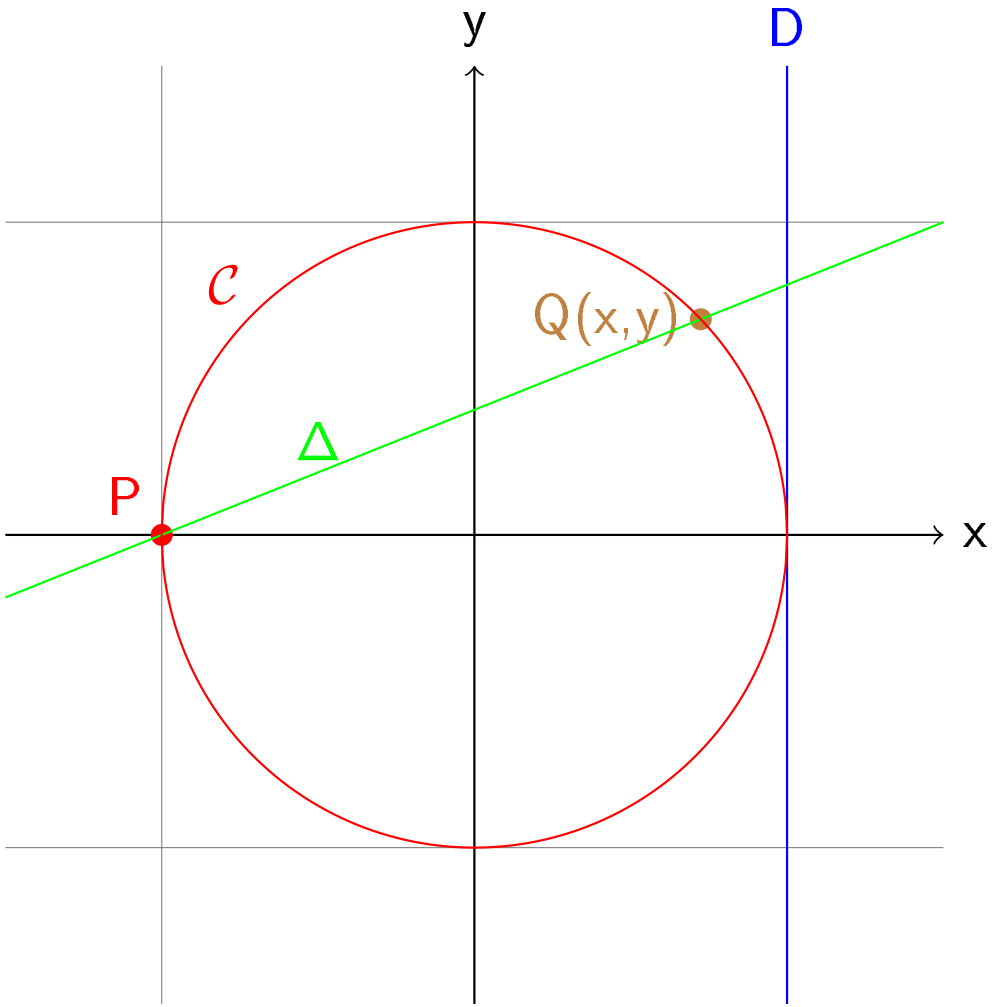
Projection stéréographique

Considérons le cercle $\mathcal{C}$ de centre l'origine et de rayon 1. Voici la figure :



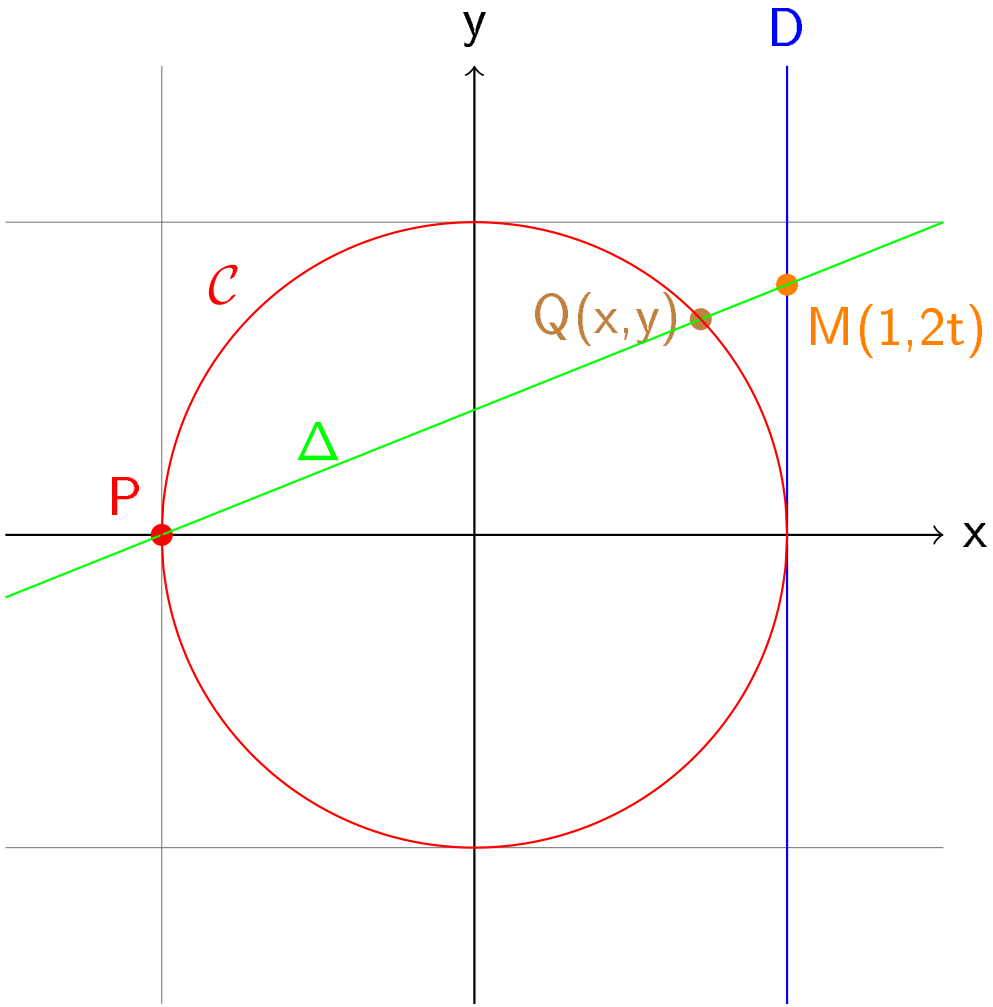
Projection stéréographique

Considérons le cercle $\mathcal{C}$ de centre l'origine et de rayon 1. Voici la figure :



Projection stéréographique

Considérons le cercle $\mathcal{C}$ de centre l'origine et de rayon 1. Voici la figure :



Correspondance cercle-droite

Si on reprend la construction précédente, on peut faire correspondre un point de D à un point de $\mathcal{C}$, et réciproquement.

Correspondance cercle-droite

Si on reprend la construction précédente, on peut faire correspondre un point de D à un point de $\mathcal{C}$, et réciproquement.

Étant donné un point $Q(x, y)$ sur le cercle $\mathcal{C}$ (autre que $P(-1, 0)$), la droite (PQ) coupe la droite D en un unique point M de coordonnées $(1, 2t)$, pour un certain t.

Correspondance cercle-droite

Si on reprend la construction précédente, on peut faire correspondre un point de D à un point de $\mathcal{C}$, et réciproquement.

Étant donné un point $Q(x, y)$ sur le cercle $\mathcal{C}$ (autre que $P(-1, 0)$), la droite (PQ) coupe la droite D en un unique point M de coordonnées $(1, 2t)$, pour un certain t.

Réciproquement, si $M \in D$ de coordonnées $(1, 2t)$, où t est un nombre réel variable,

Correspondance cercle-droite

Si on reprend la construction précédente, on peut faire correspondre un point de D à un point de $\mathcal{C}$, et réciproquement.

Étant donné un point $Q(x, y)$ sur le cercle $\mathcal{C}$ (autre que $P(-1, 0)$), la droite (PQ) coupe la droite D en un unique point M de coordonnées $(1, 2t)$, pour un certain t.

Réciproquement, si $M \in D$ de coordonnées $(1, 2t)$, où t est un nombre réel variable, la droite (PM) coupe le cercle $\mathcal{C}$ en exactement deux points :

Correspondance cercle-droite

Si on reprend la construction précédente, on peut faire correspondre un point de D à un point de $\mathcal{C}$, et réciproquement.

Étant donné un point $Q(x, y)$ sur le cercle $\mathcal{C}$ (autre que $P(-1, 0)$), la droite (PQ) coupe la droite D en un unique point M de coordonnées $(1, 2t)$, pour un certain t.

Réciproquement, si $M \in D$ de coordonnées $(1, 2t)$, où t est un nombre réel variable, la droite (PM) coupe le cercle $\mathcal{C}$ en exactement deux points : le point P et un autre point que l'on note Q, de coordonnées (x, y).

Correspondance cercle-droite

On a donc construit une "correspondance" (appelée une bijection) qui permet d'identifier le cercle $\mathcal{C}$ privé du point P avec la droite D.

Correspondance cercle-droite

On a donc construit une "correspondance" (appelée une bijection) qui permet d'identifier le cercle $\mathcal{C}$ privé du point P avec la droite D.

Géométriquement, on dit que l'on a projeté le cercle sur la droite depuis le point P : comme si on mettait une lampe au point P et un écran sur la droite D, avant de regarder l'image (l'ombre) du cercle sur l'écran.

Lien avec le problème initial

Pourquoi cela nous aide-t-il à résoudre notre problème d'arithmétique ?

Lien avec le problème initial

Pourquoi cela nous aide-t-il à résoudre notre problème d'arithmétique ?

Au lieu de chercher des points à coordonnées rationnelles sur le cercle $\mathcal{C}$, on va se ramener à chercher des points à coordonnées rationnelles sur la droite D.

Lien avec le problème initial

Pourquoi cela nous aide-t-il à résoudre notre problème d'arithmétique ?

Au lieu de chercher des points à coordonnées rationnelles sur le cercle $\mathcal{C}$, on va se ramener à chercher des points à coordonnées rationnelles sur la droite D.

C'est beaucoup plus facile, car l'équation d'une droite est de degré 1, alors que celle d'un cercle est de degré 2.

Lien avec le problème initial

Pourquoi cela nous aide-t-il à résoudre notre problème d'arithmétique ?

Au lieu de chercher des points à coordonnées rationnelles sur le cercle $\mathcal{C}$, on va se ramener à chercher des points à coordonnées rationnelles sur la droite D.

C'est beaucoup plus facile, car l'équation d'une droite est de degré 1, alors que celle d'un cercle est de degré 2.

On a besoin de vérifier que, dans la correspondance précédente entre les points de $\mathcal{C}$ et ceux de D, si un point a des coordonnées rationnelles sur $\mathcal{C}$, alors le point correspondant sur D a aussi des coordonnées rationnelles. Et réciproquement.

Question

On se pose donc la question suivante :

Question

On se pose donc la question suivante :
On rappelle la correspondance

$$\mathcal{C} \longleftrightarrow D$$

$$Q(x,y) \in \mathcal{C} \longleftrightarrow M(1,2t) \in D\,.$$

Question

On se pose donc la question suivante :
On rappelle la correspondance

$$\mathcal{C} \longleftrightarrow D$$

$$Q(x,y) \in \mathcal{C} \longleftrightarrow M(1,2t) \in D\,.$$

Question

Si x et y sont des fractions, est-ce que t est une fraction ? Et réciproquement ?

Question

On se pose donc la question suivante :
On rappelle la correspondance

$$\mathcal{C} \longleftrightarrow D$$

$$Q(x,y) \in \mathcal{C} \longleftrightarrow M(1,2t) \in D\,.$$

Question

Si x et y sont des fractions, est-ce que t est une fraction ? Et réciproquement ?

Pour cela, on a besoin de formules permettant de calculer les coordonnées de M en fonction de celles de Q. Et réciproquement.

Formules

Partons d'un point M de coordonnées $(1, 2t)$ sur D.

Formules

Partons d'un point M de coordonnées $(1, 2t)$ sur D.

L'équation de la droite (PM) s'écrit alors $y = t(x + 1)$.

Formules

Partons d'un point M de coordonnées $(1, 2t)$ sur D.

L'équation de la droite (PM) s'écrit alors $y = t(x + 1)$.

Les coordonnés (x, y) du point d'intersection Q entre la droite (PM) et $\mathcal{C}$ doivent vérifier à la fois l'équation de (PM) et celle de $\mathcal{C}$.

Formules

Partons d'un point M de coordonnées $(1, 2t)$ sur D.

L'équation de la droite (PM) s'écrit alors $y = t(x + 1)$.

Les coordonnés (x, y) du point d'intersection Q entre la droite (PM) et $\mathcal{C}$ doivent vérifier à la fois l'équation de (PM) et celle de $\mathcal{C}$.
On doit donc résoudre le système

$$\begin{cases} y = t(x+1) \\ x^2 + y^2 = 1 \end{cases}.$$

Formules

Partons d'un point M de coordonnées $(1, 2t)$ sur D.

L'équation de la droite (PM) s'écrit alors $y = t(x+1)$.

Les coordonnés (x, y) du point d'intersection Q entre la droite (PM) et $\mathcal{C}$ doivent vérifier à la fois l'équation de (PM) et celle de $\mathcal{C}$.
On doit donc résoudre le système

$$\begin{cases} y = t(x+1) \\ x^2 + y^2 = 1 \end{cases}.$$

En remplaçant y dans la seconde équation, on obtient l'équation

$$x^2 + t^2(x+1)^2 = 1\,,$$

Formules

Partons d'un point M de coordonnées $(1, 2t)$ sur D.

L'équation de la droite (PM) s'écrit alors $y = t(x+1)$.

Les coordonnés (x, y) du point d'intersection Q entre la droite (PM) et $\mathcal{C}$ doivent vérifier à la fois l'équation de (PM) et celle de $\mathcal{C}$.
On doit donc résoudre le système

$$\begin{cases} y = t(x+1) \\ x^2 + y^2 = 1 \end{cases}.$$

En remplaçant y dans la seconde équation, on obtient l'équation

$$x^2 + t^2(x+1)^2 = 1\,,$$

qui se factorise sous la forme

$$(x+1)((1+t^2)x + t^2 - 1) = 0\,.$$

On doit donc résoudre l'équation

$$(x+1)((1+t^2)x+t^2-1)=0\,.$$

On doit donc résoudre l'équation

$$(x+1)((1+t^2)x+t^2-1)=0\,.$$

Puisque $Q \neq P$, on sait que $x \neq -1$, donc l'équation précédente se réécrit $(1+t^2)x+t^2-1=0$, donc on trouve

$$x=\frac{1-t^2}{1+t^2}\,.$$

On doit donc résoudre l'équation

$$(x+1)((1+t^2)x+t^2-1)=0\,.$$

Puisque $Q \neq P$, on sait que $x \neq -1$, donc l'équation précédente se réécrit $(1+t^2)x+t^2-1=0$, donc on trouve

$$x=\frac{1-t^2}{1+t^2}\,.$$

En revenant à l'expression de y en fonction de x, on trouve alors

$$y=\frac{2t}{1+t^2}\,.$$

Formules

On a donc finalement obtenu les formules suivantes :

Formules

On a donc finalement obtenu les formules suivantes :

Si M est le point de D de coordonnées $(1, 2t)$, alors le point d'intersection entre (PM) et $\mathcal{C}$ a pour coordonnées

Formules

On a donc finalement obtenu les formules suivantes :

Si M est le point de D de coordonnées $(1, 2t)$, alors le point d'intersection entre (PM) et $\mathcal{C}$ a pour coordonnées

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

Formules

On a donc finalement obtenu les formules suivantes :

Si M est le point de D de coordonnées $(1, 2t)$, alors le point d'intersection entre (PM) et $\mathcal{C}$ a pour coordonnées

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

Dans l'autre sens, étant donné un point $Q \neq P$ sur le cercle $\mathcal{C}$ de coordonnées (x, y), alors le point M de D correspondant a pour coordonnées $(1, 2t)$, avec

$$t = \frac{y}{x+1}.$$

Formules

Finalement, en regardant les formules qui permettent de passer de la droite au cercle et celles qui permettent de passer du cercle à la droite, on constate le point crucial suivant :

Formules

Finalement, en regardant les formules qui permettent de passer de la droite au cercle et celles qui permettent de passer du cercle à la droite, on constate le point crucial suivant :

Théorème

Si Q a des coordonnées rationnelles ($x, y \in \mathbf{Q}$), alors M a des coordonnées rationnelles ($t \in Q$).

Formules

Finalement, en regardant les formules qui permettent de passer de la droite au cercle et celles qui permettent de passer du cercle à la droite, on constate le point crucial suivant :

Théorème

Si Q a des coordonnées rationnelles ($x, y \in \mathbf{Q}$), alors M a des coordonnées rationnelles ($t \in Q$).
Réciproquement, si M a des coordonnées rationnelles ($t \in \mathbf{Q}$), alors Q a des coordonnées rationnelles ($x, y \in \mathbf{Q}$).

Formules

Finalement, en regardant les formules qui permettent de passer de la droite au cercle et celles qui permettent de passer du cercle à la droite, on constate le point crucial suivant :

Théorème

Si Q a des coordonnées rationnelles ($x, y \in \mathbf{Q}$), alors M a des coordonnées rationnelles ($t \in Q$).
Réciproquement, si M a des coordonnées rationnelles ($t \in \mathbf{Q}$), alors Q a des coordonnées rationnelles ($x, y \in \mathbf{Q}$).

Donc le problème intial ("trouver les points à coordonnées rationnelles sur $\mathcal{C}$") est équivalent au nouveau problème :

Formules

Finalement, en regardant les formules qui permettent de passer de la droite au cercle et celles qui permettent de passer du cercle à la droite, on constate le point crucial suivant :

Théorème

Si Q a des coordonnées rationnelles ($x, y \in \mathbf{Q}$), alors M a des coordonnées rationnelles ($t \in Q$).
Réciproquement, si M a des coordonnées rationnelles ($t \in \mathbf{Q}$), alors Q a des coordonnées rationnelles ($x, y \in \mathbf{Q}$).

Donc le problème intial ("trouver les points à coordonnées rationnelles sur $\mathcal{C}$") est équivalent au nouveau problème :

Trouver les points à coordonnées rationnelles sur D.

Formules

Finalement, en regardant les formules qui permettent de passer de la droite au cercle et celles qui permettent de passer du cercle à la droite, on constate le point crucial suivant :

Théorème

Si Q a des coordonnées rationnelles ($x, y \in \mathbf{Q}$), alors M a des coordonnées rationnelles ($t \in Q$).
Réciproquement, si M a des coordonnées rationnelles ($t \in \mathbf{Q}$), alors Q a des coordonnées rationnelles ($x, y \in \mathbf{Q}$).

Donc le problème intial ("trouver les points à coordonnées rationnelles sur $\mathcal{C}$") est équivalent au nouveau problème :

Trouver les points à coordonnées rationnelles sur D.

Et ce nouveau problème est très simple à résoudre :

Formules

Finalement, en regardant les formules qui permettent de passer de la droite au cercle et celles qui permettent de passer du cercle à la droite, on constate le point crucial suivant :

Théorème

Si Q a des coordonnées rationnelles ($x, y \in \mathbf{Q}$), alors M a des coordonnées rationnelles ($t \in Q$).
Réciproquement, si M a des coordonnées rationnelles ($t \in \mathbf{Q}$), alors Q a des coordonnées rationnelles ($x, y \in \mathbf{Q}$).

Donc le problème intial ("trouver les points à coordonnées rationnelles sur $\mathcal{C}$") est équivalent au nouveau problème :

Trouver les points à coordonnées rationnelles sur D.

Et ce nouveau problème est très simple à résoudre : les points à coordonnées rationnelles sur D sont exactement les points M de coordonnés $(1, 2t)$, avec $t \in \mathbf{Q}$.

Points rationnels sur le cercle

Revenons à nos moutons : quels sont les points rationnels sur le cercle $\mathcal{C}$?

Points rationnels sur le cercle

Revenons à nos moutons : quels sont les points rationnels sur le cercle $\mathcal{C}$?

Au point M de coordonnées $(1, 2t)$ sur $\mathcal{C}$ (avec $t \in \mathbf{Q}$) correspond le point $Q(x, y)$ sur $\mathcal{C}$ avec

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

Points rationnels sur le cercle

Revenons à nos moutons : quels sont les points rationnels sur le cercle $\mathcal{C}$?

Au point M de coordonnées $(1, 2t)$ sur $\mathcal{C}$ (avec $t \in \mathbf{Q}$) correspond le point $Q(x, y)$ sur $\mathcal{C}$ avec

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

On sait donc que les points recherchés sont les points de coordonnées

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

où t est une fraction quelconque.

Points rationnels sur le cercle

Revenons à nos moutons : quels sont les points rationnels sur le cercle $\mathcal{C}$?

Au point M de coordonnées $(1, 2t)$ sur $\mathcal{C}$ (avec $t \in \mathbf{Q}$) correspond le point $Q(x, y)$ sur $\mathcal{C}$ avec

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

On sait donc que les points recherchés sont les points de coordonnées

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

où t est une fraction quelconque.
Par exemple, pour $t = \frac{1}{2}$, on retrouve le point de coordonnées $(\frac{3}{5}, \frac{4}{5})$.

Points rationnels sur le cercle

Revenons à nos moutons : quels sont les points rationnels sur le cercle $\mathcal{C}$?

Au point M de coordonnées $(1, 2t)$ sur $\mathcal{C}$ (avec $t \in \mathbf{Q}$) correspond le point $Q(x, y)$ sur $\mathcal{C}$ avec

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

On sait donc que les points recherchés sont les points de coordonnées

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

où t est une fraction quelconque.
Par exemple, pour $t = \frac{1}{2}$, on retrouve le point de coordonnées $(\frac{3}{5}, \frac{4}{5})$.
Pour $t = \frac{2}{3}$, on trouve le point $(\frac{5}{13}, \frac{12}{13})$.

Points rationnels sur le cercle

Revenons à nos moutons : quels sont les points rationnels sur le cercle $\mathcal{C}$?

Au point M de coordonnées $(1, 2t)$ sur $\mathcal{C}$ (avec $t \in \mathbf{Q}$) correspond le point $Q(x, y)$ sur $\mathcal{C}$ avec

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

On sait donc que les points recherchés sont les points de coordonnées

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

où t est une fraction quelconque.
Par exemple, pour $t = \frac{1}{2}$, on retrouve le point de coordonnées $(\frac{3}{5}, \frac{4}{5})$.
Pour $t = \frac{2}{3}$, on trouve le point $(\frac{5}{13}, \frac{12}{13})$.
On a donc résolu le problème de trouver tous les points rationnels sur le cercle $\mathcal{C}$.

Problème de Pythagore

Il nous reste maintenant à revenir au problème initial, à savoir trouver les solutions entières de l'équation $x^2 + y^2 = z^2$.

Problème de Pythagore

Il nous reste maintenant à revenir au problème initial, à savoir trouver les solutions entières de l'équation $x^2 + y^2 = z^2$.

Pour passer d'une solution entière de ce problème à un point rationnel du cercle, on a divisé x et y par z.

Problème de Pythagore

Il nous reste maintenant à revenir au problème initial, à savoir trouver les solutions entières de l'équation $x^2 + y^2 = z^2$.

Pour passer d'une solution entière de ce problème à un point rationnel du cercle, on a divisé x et y par z.
On a besoin de l'opération inverse : on connaît les points rationnels du cercle, on veut en déduire les solutions de problème de Pythagore.

Problème de Pythagore

Il nous reste maintenant à revenir au problème initial, à savoir trouver les solutions entières de l'équation $x^2 + y^2 = z^2$.

Pour passer d'une solution entière de ce problème à un point rationnel du cercle, on a divisé x et y par z.
On a besoin de l'opération inverse : on connaît les points rationnels du cercle, on veut en déduire les solutions de problème de Pythagore.

Pour cela, on part d'un point du cercle de coordonnées (x, y), avec $x = \frac{a}{c}$ et $y = \frac{b}{c}$ des fractions : on a $x^2 + y^2 = 1$, c'est-à-dire $\frac{a^2}{c^2} + \frac{b^2}{c^2} = 1$.

Problème de Pythagore

Il nous reste maintenant à revenir au problème initial, à savoir trouver les solutions entières de l'équation $x^2 + y^2 = z^2$.

Pour passer d'une solution entière de ce problème à un point rationnel du cercle, on a divisé x et y par z.
On a besoin de l'opération inverse : on connaît les points rationnels du cercle, on veut en déduire les solutions de problème de Pythagore.

Pour cela, on part d'un point du cercle de coordonnées (x, y), avec $x = \frac{a}{c}$ et $y = \frac{b}{c}$ des fractions : on a $x^2 + y^2 = 1$, c'est-à-dire $\frac{a^2}{c^2} + \frac{b^2}{c^2} = 1$.

Alors la solution correspondante au problème de Pythagore est le triplet d'entiers (a, b, c), qui vérifie bien $a^2 + b^2 = c^2$.

Solutions du problème de Pythagore

Vu les raisonnements précédents, on sait que toutes les solutions du problème de Pythagore sont de la forme obtenue à la page précédente.

Solutions du problème de Pythagore

Vu les raisonnements précédents, on sait que toutes les solutions du problème de Pythagore sont de la forme obtenue à la page précédente.

Or on sait que si (x, y) est un point rationnel de $\mathcal{C}$, alors il est donné par une fraction $t = \frac{u}{v}$ telle que

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

Solutions du problème de Pythagore

Vu les raisonnements précédents, on sait que toutes les solutions du problème de Pythagore sont de la forme obtenue à la page précédente.

Or on sait que si (x, y) est un point rationnel de $\mathcal{C}$, alors il est donné par une fraction $t = \frac{u}{v}$ telle que

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

Cela se réécrit (en remplaçant t par $\frac{u}{v}$) :

$$\begin{cases} x = \frac{v^2-u^2}{v^2+u^2} \\ y = \frac{2uv}{v^2+u^2} \end{cases}.$$

Solutions du problème de Pythagore

Vu les raisonnements précédents, on sait que toutes les solutions du problème de Pythagore sont de la forme obtenue à la page précédente.

Or on sait que si (x, y) est un point rationnel de $\mathcal{C}$, alors il est donné par une fraction $t = \frac{u}{v}$ telle que

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

Cela se réécrit (en remplaçant t par $\frac{u}{v}$) :

$$\begin{cases} x = \frac{v^2-u^2}{v^2+u^2} \\ y = \frac{2uv}{v^2+u^2} \end{cases}.$$

Donc la solution correspondante au problème de Pythagore est :

$$\begin{cases} a = v^2 - u^2 \\ b = 2uv \\ c = v^2 + u^2 \end{cases}.$$

Enfin la solution !

On est enfin parvenu à résoudre la problème initial !

Enfin la solution !

On est enfin parvenu à résoudre la problème initial !
Les triplets d'entiers (a, b, c) vérifiant $a^2 + b^2 = c^2$ sont exactement les entiers de la forme

$$\begin{cases} a = v^2 - u^2 \\ b = 2uv \\ c = v^2 + u^2 \end{cases},$$

où u et v sont deux entiers quelconques.

Enfin la solution !

On est enfin parvenu à résoudre la problème initial !
Les triplets d'entiers (a, b, c) vérifiant $a^2 + b^2 = c^2$ sont exactement les entiers de la forme

$$\begin{cases} a = v^2 - u^2 \\ b = 2uv \\ c = v^2 + u^2 \end{cases},$$

où u et v sont deux entiers quelconques.

On voit notamment que le problème initial admet donc une infinité de solutions vraiment différentes, et on a la liste complète de toutes les solutions.

Exemples de solutions

On applique la formule obtenue :

Exemples de solutions

On applique la formule obtenue :

$$\begin{cases} a = v^2 - u^2 \\ b = 2uv \\ c = v^2 + u^2 \end{cases},$$

où u et v sont deux entiers quelconques.

Exemples de solutions

On applique la formule obtenue :

$$\begin{cases} a = v^2 - u^2 \\ b = 2uv \\ c = v^2 + u^2 \end{cases},$$

où u et v sont deux entiers quelconques.

Par exemple, en prenant $(u, v) = (1, 2)$, on obtient le triplet $(3, 4, 5)$.

Exemples de solutions

On applique la formule obtenue :

$$\begin{cases} a = v^2 - u^2 \\ b = 2uv \\ c = v^2 + u^2 \end{cases},$$

où u et v sont deux entiers quelconques.

Par exemple, en prenant $(u, v) = (1, 2)$, on obtient le triplet $(3, 4, 5)$.

En prenant $(u, v) = (1, 4)$, on obtient le triplet $(15, 8, 16)$.

Exemples de solutions

On applique la formule obtenue :

$$\begin{cases} a = v^2 - u^2 \\ b = 2uv \\ c = v^2 + u^2 \end{cases},$$

où u et v sont deux entiers quelconques.

Par exemple, en prenant $(u, v) = (1, 2)$, on obtient le triplet $(3, 4, 5)$.

En prenant $(u, v) = (1, 4)$, on obtient le triplet $(15, 8, 16)$.

En prenant $(u, v) = (2, 3)$, on obtient le triplet $(5, 12, 13)$.

Exemples de solutions

On applique la formule obtenue :

$$\begin{cases} a = v^2 - u^2 \\ b = 2uv \\ c = v^2 + u^2 \end{cases},$$

où u et v sont deux entiers quelconques.

Par exemple, en prenant $(u, v) = (1, 2)$, on obtient le triplet $(3, 4, 5)$.

En prenant $(u, v) = (1, 4)$, on obtient le triplet $(15, 8, 16)$.

En prenant $(u, v) = (2, 3)$, on obtient le triplet $(5, 12, 13)$.

En prenant $(u, v) = (4, 9)$, on obtient le triplet $(65, 72, 97)$. On en déduit la jolie formule

$$65^2 + 72^2 = 97^2 .$$

Exemples de solutions

On applique la formule obtenue :

$$\begin{cases} a = v^2 - u^2 \\ b = 2uv \\ c = v^2 + u^2 \end{cases},$$

où u et v sont deux entiers quelconques.

Par exemple, en prenant $(u, v) = (1, 2)$, on obtient le triplet $(3, 4, 5)$.

En prenant $(u, v) = (1, 4)$, on obtient le triplet $(15, 8, 16)$.

En prenant $(u, v) = (2, 3)$, on obtient le triplet $(5, 12, 13)$.

En prenant $(u, v) = (4, 9)$, on obtient le triplet $(65, 72, 97)$. On en déduit la jolie formule

$$65^2 + 72^2 = 97^2 .$$

En prenant $(u, v) = (314, 1729)$, on obtient le triplet $(2890845, 1085812, 3088037)$. On en déduit la jolie formule

$$2890845^2 + 1085812^2 = 3088037^2 .$$

Une application

On peut utiliser le résultat sur les triplets pythagoriciens (les solutions entières de $x^2 + y^2 = z^2$) pour montrer le

Une application

On peut utiliser le résultat sur les triplets pythagoriciens (les solutions entières de $x^2 + y^2 = z^2$) pour montrer le

Théorème

L'équation $x^4 + y^4 = z^4$ n'admet aucune solution en nombres entiers non nuls.

Une application

On peut utiliser le résultat sur les triplets pythagoriciens (les solutions entières de $x^2 + y^2 = z^2$) pour montrer le

Théorème

L'équation $x^4 + y^4 = z^4$ n'admet aucune solution en nombres entiers non nuls.

Idée de la preuve : on fait un raisonnement par l'absurde. Supposons que l'on ait trois entiers x, y, z non nuls vérifiant l'équation $x^4 + y^4 = z^2$.

Une application

On peut utiliser le résultat sur les triplets pythagoriciens (les solutions entières de $x^2 + y^2 = z^2$) pour montrer le

Théorème

L'équation $x^4 + y^4 = z^4$ n'admet aucune solution en nombres entiers non nuls.

Idée de la preuve : on fait un raisonnement par l'absurde. Supposons que l'on ait trois entiers x, y, z non nuls vérifiant l'équation $x^4 + y^4 = z^2$.

On peut supposer que x et y n'ont pas de facteur commun. Alors (x^2, y^2, z) est un triplet pythagoricien.

Une application

On peut utiliser le résultat sur les triplets pythagoriciens (les solutions entières de $x^2 + y^2 = z^2$) pour montrer le

Théorème

L'équation $x^4 + y^4 = z^4$ n'admet aucune solution en nombres entiers non nuls.

Idée de la preuve : on fait un raisonnement par l'absurde. Supposons que l'on ait trois entiers x, y, z non nuls vérifiant l'équation $x^4 + y^4 = z^2$.

On peut supposer que x et y n'ont pas de facteur commun. Alors (x^2, y^2, z) est un triplet pythagoricien.

Donc par le résultat précédent, on peut trouver des entiers $u, v \in \mathbf{Z}$ tels que

$$\begin{cases} x^2 = v^2 - u^2 \\ y^2 = 2uv \\ z = v^2 + u^2 \end{cases}.$$

Suite de la preuve

En particulier, la première équation se réécrit

$$x^2 + u^2 = v^2$$

donc (x, u, v) est un triplet pythagoricien.

Suite de la preuve

En particulier, la première équation se réécrit

$$x^2 + u^2 = v^2$$

donc (x, u, v) est un triplet pythagoricien.

Donc on peut trouver des entiers $a, b \in \mathbf{Z}$ tels que

$$\begin{cases} x = b^2 - a^2 \\ u = 2ab \\ v = b^2 + a^2 \end{cases}.$$

Suite de la preuve

En particulier, la première équation se réécrit

$$x^2 + u^2 = v^2$$

donc (x, u, v) est un triplet pythagoricien.

Donc on peut trouver des entiers $a, b \in \mathbf{Z}$ tels que

$$\begin{cases} x = b^2 - a^2 \\ u = 2ab \\ v = b^2 + a^2 \end{cases}.$$

On en déduit que $y^2 = 4abv$. Puisque x et y n'ont pas de facteurs communs, on sait a, b et v n'ont pas non plus de facteur commun deux à deux.

Suite de la preuve

En particulier, la première équation se réécrit

$$x^2 + u^2 = v^2$$

donc (x, u, v) est un triplet pythagoricien.

Donc on peut trouver des entiers $a, b \in \mathbf{Z}$ tels que

$$\begin{cases} x = b^2 - a^2 \\ u = 2ab \\ v = b^2 + a^2 \end{cases}.$$

On en déduit que $y^2 = 4abv$. Puisque x et y n'ont pas de facteurs communs, on sait a, b et v n'ont pas non plus de facteur commun deux à deux.

On en déduit que a, b et v sont des carrés parfaits : il existe des entiers $c, d, e \in \mathbf{Z}$ tels que $a = c^2$, $b = d^2$ et $v = e^2$.

Suite de la preuve

Alors l'égalité $v = b^2 + a^2$ devient $e^2 = c^4 + d^4$, donc (c, d, e) est aussi solution de l'équation $x^4 + y^4 = z^2$ et par construction $0 < e < z$.

Suite de la preuve

Alors l'égalité $v = b^2 + a^2$ devient $e^2 = c^4 + d^4$, donc (c, d, e) est aussi solution de l'équation $x^4 + y^4 = z^2$ et par construction $0 < e < z$.

On peut alors recommencer une infinité de fois cette construction et construire des solutions entières positives de plus en plus petites de l'équation $x^4 + y^4 = z^2$.

Suite de la preuve

Alors l'égalité $v = b^2 + a^2$ devient $e^2 = c^4 + d^4$, donc (c, d, e) est aussi solution de l'équation $x^4 + y^4 = z^2$ et par construction $0 < e < z$.

On peut alors recommencer une infinité de fois cette construction et construire des solutions entières positives de plus en plus petites de l'équation $x^4 + y^4 = z^2$.

Ceci est IMPOSSIBLE car on ne peut pas construire une suite infinie d'entiers positifs de plus en plus petits...

Suite de la preuve

Alors l'égalité $v = b^2 + a^2$ devient $e^2 = c^4 + d^4$, donc (c, d, e) est aussi solution de l'équation $x^4 + y^4 = z^2$ et par construction $0 < e < z$.

On peut alors recommencer une infinité de fois cette construction et construire des solutions entières positives de plus en plus petites de l'équation $x^4 + y^4 = z^2$.

Ceci est IMPOSSIBLE car on ne peut pas construire une suite infinie d'entiers positifs de plus en plus petits...

Cette contradiction nous dit que l'hypothèse initiale est fausse, donc l'équation $x^4 + y^4 = z^2$ n'a pas de solution entière non triviale.

Suite de la preuve

Alors l'égalité $v = b^2 + a^2$ devient $e^2 = c^4 + d^4$, donc (c, d, e) est aussi solution de l'équation $x^4 + y^4 = z^2$ et par construction $0 < e < z$.

On peut alors recommencer une infinité de fois cette construction et construire des solutions entières positives de plus en plus petites de l'équation $x^4 + y^4 = z^2$.

Ceci est IMPOSSIBLE car on ne peut pas construire une suite infinie d'entiers positifs de plus en plus petits...

Cette contradiction nous dit que l'hypothèse initiale est fausse, donc l'équation $x^4 + y^4 = z^2$ n'a pas de solution entière non triviale.

Cela termine la preuve du théorème

Généralisations

La méthode géométrique du "dépliage du cercle" s'applique de la même façon pour trouver les solutions entières d'équations de la forme

Généralisations

La méthode géométrique du "dépliage du cercle" s'applique de la même façon pour trouver les solutions entières d'équations de la forme

$$ax^2 + by^2 + cz^2 = 0\,,$$

où a, b, c sont trois entiers fixés.

Généralisations

La méthode géométrique du "dépliage du cercle" s'applique de la même façon pour trouver les solutions entières d'équations de la forme

$$ax^2 + by^2 + cz^2 = 0\,,$$

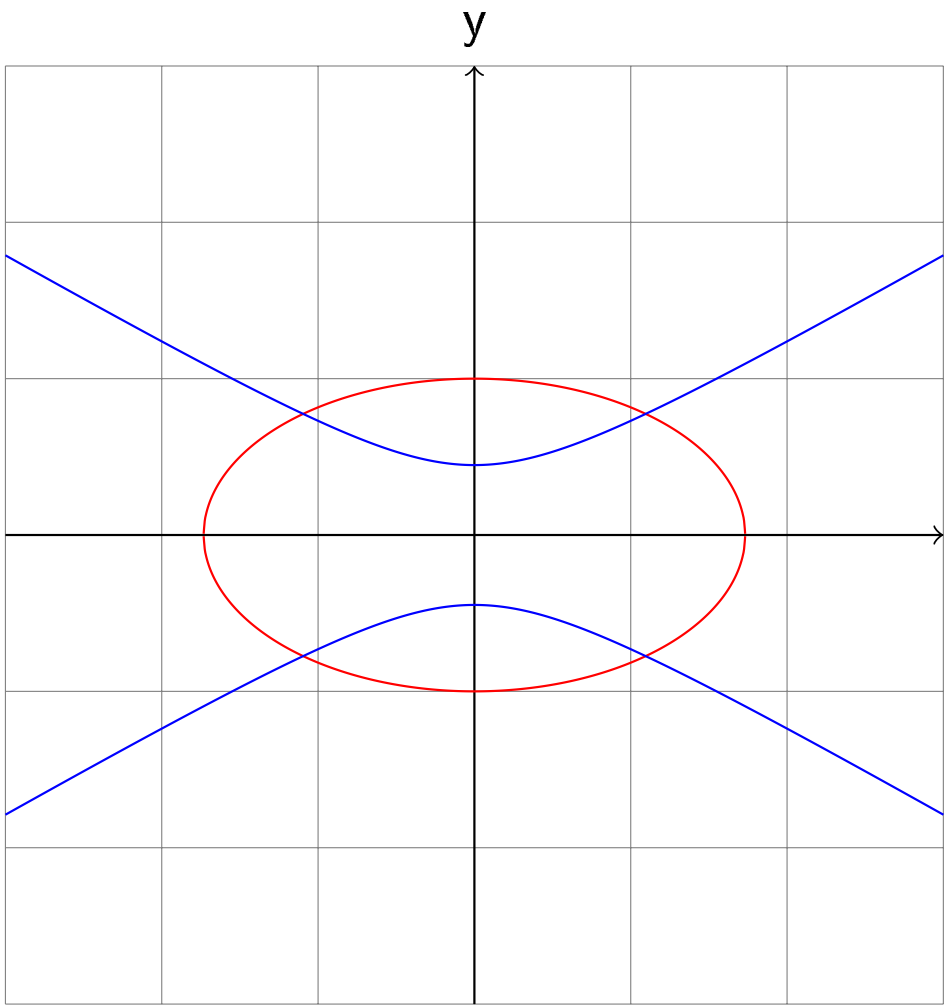
où a, b, c sont trois entiers fixés.

Géométriquement, en divisant par z^2, on obtient une courbe d'équation

$$aX^2 + bY^2 = -c\,.$$

Suivant les valeurs de a, b, c, la courbe est soit une ellipse, soit une hyperbole :

Figures : ellipse et hyperbole



$\frac{x^2}{3} + y^2 = -0,2$

$\frac{x^2}{3} + y^2 = 1$

Généralisations

Dans tous ces cas, si on trouve une solution entière (i.e. un point sur la courbe à coordonnées rationnelles), alors la courbe est en correspondance avec une droite et le problème est résolu.

Généralisations

Dans tous ces cas, si on trouve une solution entière (i.e. un point sur la courbe à coordonnées rationnelles), alors la courbe est en correspondance avec une droite et le problème est résolu.

La difficulté est donc ici de savoir si il y a au moins un point rationnel.

Généralisations

Dans tous ces cas, si on trouve une solution entière (i.e. un point sur la courbe à coordonnées rationnelles), alors la courbe est en correspondance avec une droite et le problème est résolu.

La difficulté est donc ici de savoir si il y a au moins un point rationnel.

On dispose d'un algorithme pour savoir si une telle équation admet au moins une solution. Voici quelques exemples :

Généralisations

Dans tous ces cas, si on trouve une solution entière (i.e. un point sur la courbe à coordonnées rationnelles), alors la courbe est en correspondance avec une droite et le problème est résolu.

La difficulté est donc ici de savoir si il y a au moins un point rationnel.

On dispose d'un algorithme pour savoir si une telle équation admet au moins une solution. Voici quelques exemples :

Exemple :

1. L'équation $3x^2 + 5y^2 = -2$ n'a pas de solution réelle (problème de signe).

Généralisations

Dans tous ces cas, si on trouve une solution entière (i.e. un point sur la courbe à coordonnées rationnelles), alors la courbe est en correspondance avec une droite et le problème est résolu.

La difficulté est donc ici de savoir si il y a au moins un point rationnel.

On dispose d'un algorithme pour savoir si une telle équation admet au moins une solution. Voici quelques exemples :

Exemple :

1. L'équation $3x^2 + 5y^2 = -2$ n'a pas de solution réelle (problème de signe).
2. L'équation $x^2 - 2y^2 = 0$ n'a pas de solution rationnelle autre que $(0, 0)$ (divisibilité par 2 et $\sqrt{2}$ n'est pas une fraction).

Généralisations

Dans tous ces cas, si on trouve une solution entière (i.e. un point sur la courbe à coordonnées rationnelles), alors la courbe est en correspondance avec une droite et le problème est résolu.

La difficulté est donc ici de savoir si il y a au moins un point rationnel.

On dispose d'un algorithme pour savoir si une telle équation admet au moins une solution. Voici quelques exemples :

Exemple :

1. L'équation $3x^2 + 5y^2 = -2$ n'a pas de solution réelle (problème de signe).
2. L'équation $x^2 - 2y^2 = 0$ n'a pas de solution rationnelle autre que $(0, 0)$ (divisibilité par 2 et $\sqrt{2}$ n'est pas une fraction).
3. L'équation $x^2 + y^2 = 3$ n'a pas de solution rationnelle (divisibilité par 3 et $\sqrt{3}$ n'est pas une fraction).

Généralisations

Dans tous ces cas, si on trouve une solution entière (i.e. un point sur la courbe à coordonnées rationnelles), alors la courbe est en correspondance avec une droite et le problème est résolu.

La difficulté est donc ici de savoir si il y a au moins un point rationnel.

On dispose d'un algorithme pour savoir si une telle équation admet au moins une solution. Voici quelques exemples :

Exemple :

1. L'équation $3x^2 + 5y^2 = -2$ n'a pas de solution réelle (problème de signe).
2. L'équation $x^2 - 2y^2 = 0$ n'a pas de solution rationnelle autre que $(0, 0)$ (divisibilité par 2 et $\sqrt{2}$ n'est pas une fraction).
3. L'équation $x^2 + y^2 = 3$ n'a pas de solution rationnelle (divisibilité par 3 et $\sqrt{3}$ n'est pas une fraction).
4. L'équation $x^2 - 3y^2 = 3$ a une infinité de solutions rationnelles.

Avec plus d'inconnues ?

De la même façon, si on augmente le nombre d'inconnues, on dispose d'algorithmes (datant du début du 20ème siècle) pour trouver les solutions entières (ou rationnelles) des équations de degré 2.

Avec plus d'inconnues ?

De la même façon, si on augmente le nombre d'inconnues, on dispose d'algorithmes (datant du début du 20ème siècle) pour trouver les solutions entières (ou rationnelles) des équations de degré 2.

Théorème (Hasse-Minkowski 1924)

On sait déterminer si une équation de la forme

$$a_1 x_1^2 + a_2 x_2^2 + \cdots + a_n x_n^2 = c$$

a des solutions entières ou rationnelles.

Avec plus d'inconnues ?

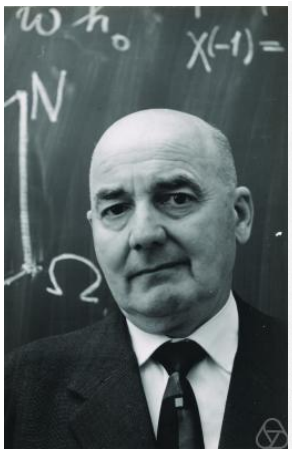
De la même façon, si on augmente le nombre d'inconnues, on dispose d'algorithmes (datant du début du 20ème siècle) pour trouver les solutions entières (ou rationnelles) des équations de degré 2.

Théorème (Hasse-Minkowski 1924)

On sait déterminer si une équation de la forme

$$a_1 x_1^2 + a_2 x_2^2 + \cdots + a_n x_n^2 = c$$

a des solutions entières ou rationnelles.



Généralisations du problème de Pythagore

Suite à la résolution des problèmes précédents, les mathématiciens se sont intéressés à d'autres généralisations de ces équations.

Généralisations du problème de Pythagore

Suite à la résolution des problèmes précédents, les mathématiciens se sont intéressés à d'autres généralisations de ces équations.

En particulier, ils ont cherché à trouver les solutions entières des équations

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

avec $n \geq 1$ entier fixé.

Généralisations du problème de Pythagore

Suite à la résolution des problèmes précédents, les mathématiciens se sont intéressés à d'autres généralisations de ces équations.

En particulier, ils ont cherché à trouver les solutions entières des équations

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

avec $n \geq 1$ entier fixé.

Le cas $n = 1$ est très simple, le cas $n = 2$ est le problème de Pythagore (infinité de solutions, avec liste complète des solutions). On a montré que le cas $n = 4$ n'avait pas de solutions non nulles.

Généralisations du problème de Pythagore

Suite à la résolution des problèmes précédents, les mathématiciens se sont intéressés à d'autres généralisations de ces équations.

En particulier, ils ont cherché à trouver les solutions entières des équations

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

avec $n \geq 1$ entier fixé.

Le cas $n = 1$ est très simple, le cas $n = 2$ est le problème de Pythagore (infinité de solutions, avec liste complète des solutions). On a montré que le cas $n = 4$ n'avait pas de solutions non nulles.

La question suivante est donc très naturelle :

Le "théorème" de Fermat

Question (Fermat 1641)

Fixons $n \geq 3$. Quelles sont les solutions entières non nulles de l'équation

$$x^n + y^n = z^n \, ?$$

Le "théorème" de Fermat

Question (Fermat 1641)

Fixons $n \geq 3$. Quelles sont les solutions entières non nulles de l'équation

$$x^n + y^n = z^n \, ?$$

Fermat est persuadé qu'il n'y a aucune solution entière non nulle.

Le "théorème" de Fermat

Question (Fermat 1641)

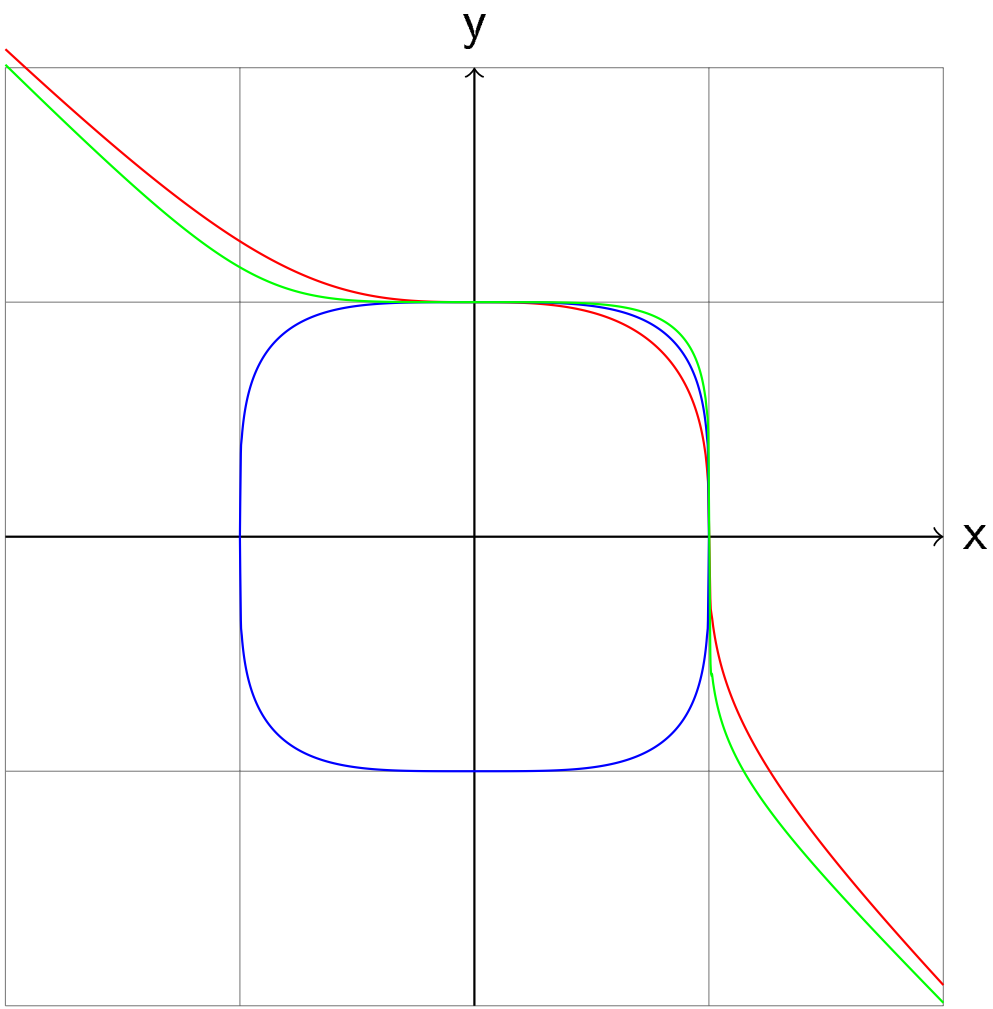
Fixons $n \geq 3$. Quelles sont les solutions entières non nulles de l'équation

$$x^n + y^n = z^n \, ?$$

Fermat est persuadé qu'il n'y a aucune solution entière non nulle.

Géométrie des équations de Fermat

Les dessins dans les cas $n = 3$, $n = 4$ et $n = 5$ sont les suivants :



n=3

n=4

n=5

Solutions ?

La réponse à cette question est BEAUCOUP plus difficile que les cas $n = 1, 2$ ou 4 étudiés auparavant.

Solutions ?

La réponse à cette question est BEAUCOUP plus difficile que les cas $n = 1, 2$ ou 4 étudiés auparavant.

Pour certaines valeurs de n, on a réussi à démontrer petit à petit qu'il n'y avait pas de solutions :

Solutions ?

La réponse à cette question est BEAUCOUP plus difficile que les cas $n = 1, 2$ ou 4 étudiés auparavant.

Pour certaines valeurs de n, on a réussi à démontrer petit à petit qu'il n'y avait pas de solutions :

Fermat (1641, $n = 4$), Euler (1753, $n = 3$), Gauss (1801, $n = 3$), Sophie Germain (1825, plusieurs n), etc...

Solutions ?

La réponse à cette question est BEAUCOUP plus difficile que les cas $n = 1, 2$ ou 4 étudiés auparavant.

Pour certaines valeurs de n, on a réussi à démontrer petit à petit qu'il n'y avait pas de solutions :

Fermat (1641, $n = 4$), Euler (1753, $n = 3$), Gauss (1801, $n = 3$), Sophie Germain (1825, plusieurs n), etc...

Andrew Wiles

La solution générale a finalement attendu plus de trois siècles :

Andrew Wiles

La solution générale a finalement attendu plus de trois siècles :

Théorème (Wiles 1995)

Si $n \geq 3$, l'équation

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

n'admet pas de solution entière non triviale.

Andrew Wiles

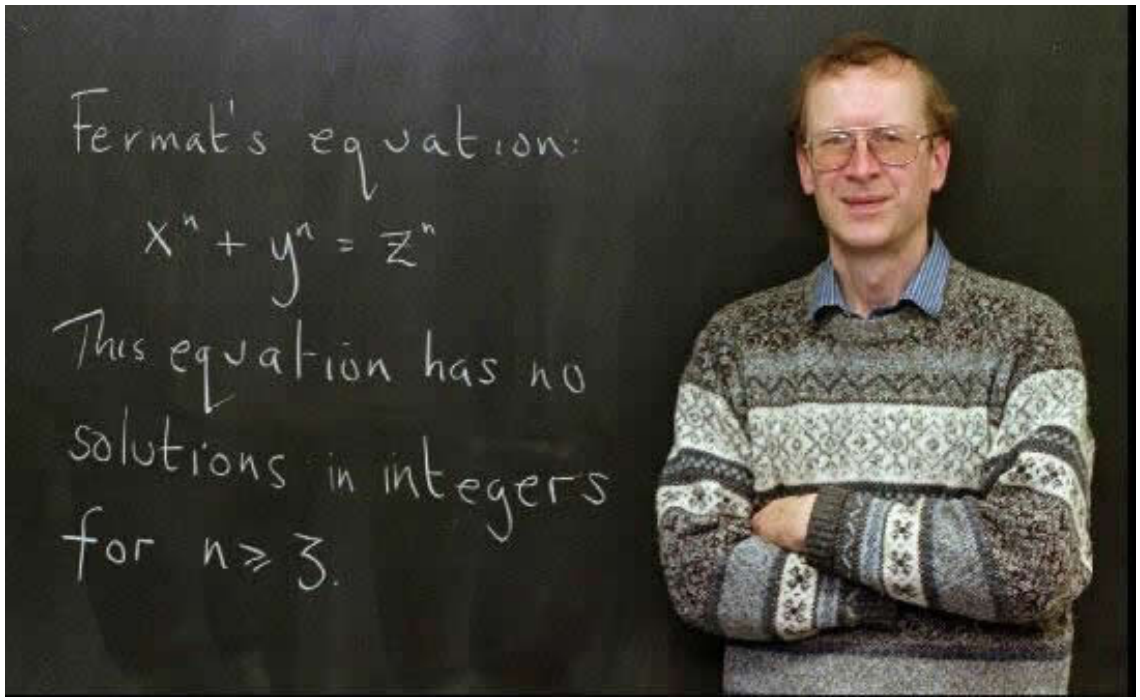
La solution générale a finalement attendu plus de trois siècles :

Théorème (Wiles 1995)

Si $n \geq 3$, l'équation

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

n'admet pas de solution entière non triviale.



Retour sur Terre

Revenons à des problèmes plus simples que le théorème de Fermat-Wiles.

Retour sur Terre

Revenons à des problèmes plus simples que le théorème de Fermat-Wiles.

On a vu que l'arithmétique et la géométrie élémentaires permettaient de résoudre complétement les équations en nombres entiers de degré 1 et 2.

Retour sur Terre

Revenons à des problèmes plus simples que le théorème de Fermat-Wiles.

On a vu que l'arithmétique et la géométrie élémentaires permettaient de résoudre complétement les équations en nombres entiers de degré 1 et 2.

La question naturelle qui se pose alors est : "que se passe-t-il en degré supérieur ?"

Retour sur Terre

Revenons à des problèmes plus simples que le théorème de Fermat-Wiles.

On a vu que l'arithmétique et la géométrie élémentaires permettaient de résoudre complétement les équations en nombres entiers de degré 1 et 2.

La question naturelle qui se pose alors est : "que se passe-t-il en degré supérieur ?"

La réponse est très compliquée dans le cas général. On va donc d'abord se concentrer sur un type d'équation particulier :

Équations de degré 3

On considère une équation de degré 3 avec deux inconnues, de la forme

$$y^2 = x^3 + ax + b\,,$$

où $a, b \in Z$ sont fixés.

Équations de degré 3

On considère une équation de degré 3 avec deux inconnues, de la forme

$$y^2 = x^3 + ax + b\,,$$

où $a, b \in Z$ sont fixés.

Comme précédemment, on peut associer à une telle équation une courbe, correspondant à tous les points du plan dont les coordonnées (x, y) vérifient l'équation.

Équations de degré 3

On considère une équation de degré 3 avec deux inconnues, de la forme

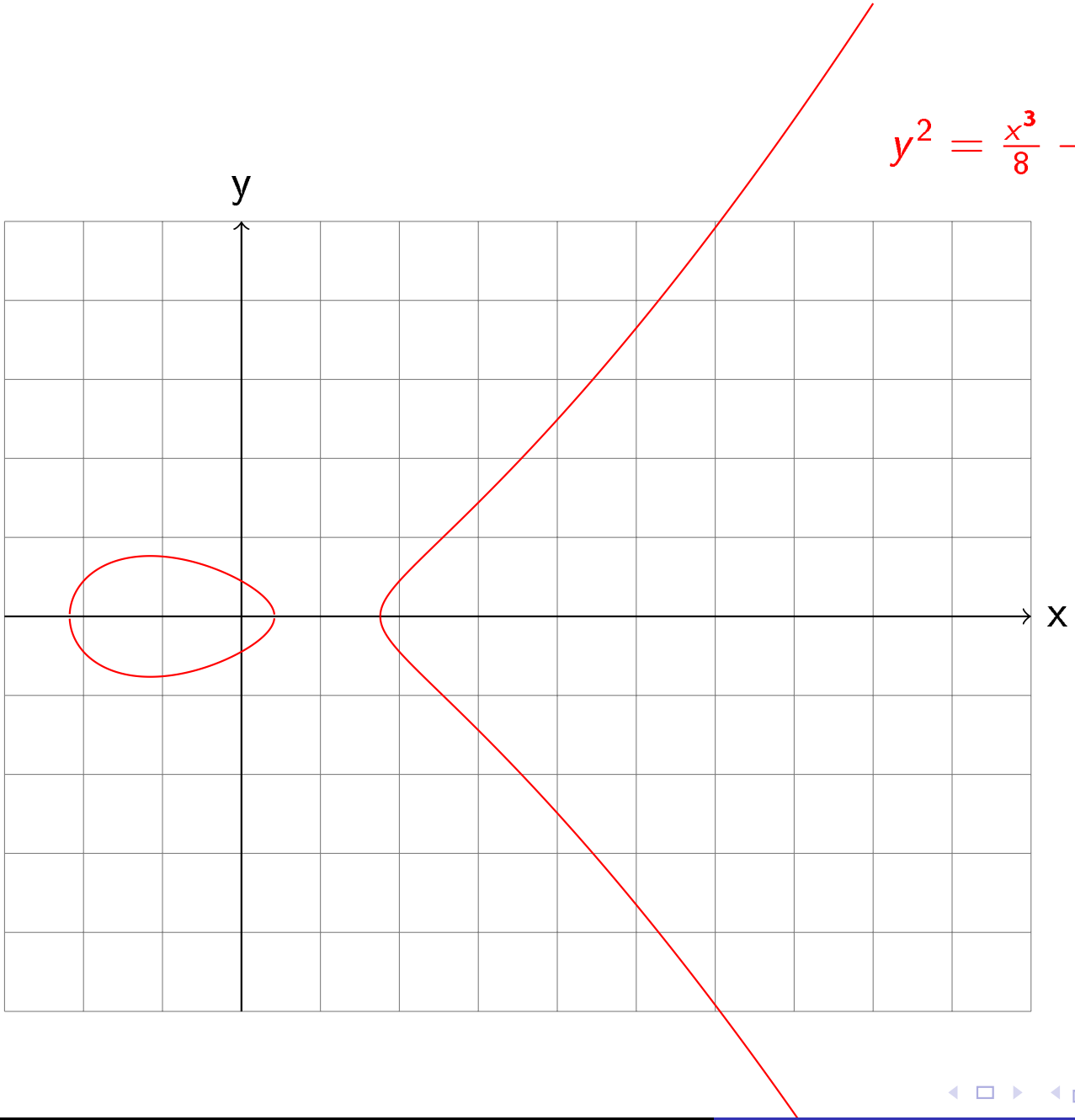
$$y^2 = x^3 + ax + b\,,$$

où $a, b \in Z$ sont fixés.

Comme précédemment, on peut associer à une telle équation une courbe, correspondant à tous les points du plan dont les coordonnées (x, y) vérifient l'équation.

Le problème arithmétique qui consiste à trouver les solutions entières ou rationnelles de l'équation se traduit géométriquement par la recherche des points à coordonnées entières ou rationnelles sur cette courbe.

Une courbe de degré 3



Courbes elliptiques

Comme avec le cercle, on peut essayer de couper la courbe avec une droite.

Courbes elliptiques

Comme avec le cercle, on peut essayer de couper la courbe avec une droite.

Dans le cas du cercle, une droite coupait le cercle en exactement deux points. Dans le cas présent, on voit qu'une droite coupe la courbe en exactement trois points (en général).

Courbes elliptiques

Comme avec le cercle, on peut essayer de couper la courbe avec une droite.

Dans le cas du cercle, une droite coupait le cercle en exactement deux points. Dans le cas présent, on voit qu'une droite coupe la courbe en exactement trois points (en général).

En effet, une équation de degré 2 en une variable admet deux solutions, une équation de degré 3 admet trois solutions.

Courbes elliptiques

Comme avec le cercle, on peut essayer de couper la courbe avec une droite.

Dans le cas du cercle, une droite coupait le cercle en exactement deux points. Dans le cas présent, on voit qu'une droite coupe la courbe en exactement trois points (en général).

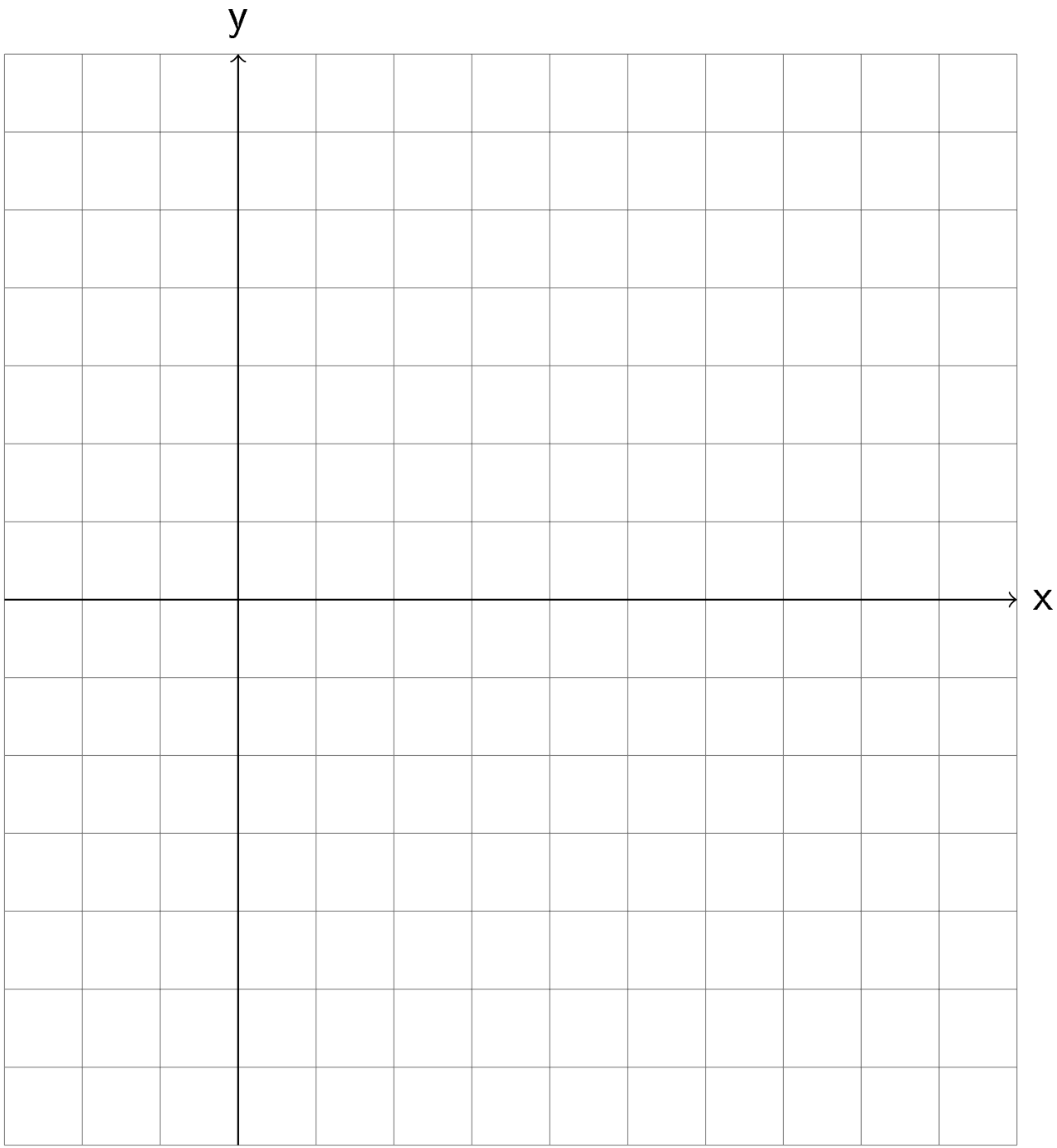
En effet, une équation de degré 2 en une variable admet deux solutions, une équation de degré 3 admet trois solutions.

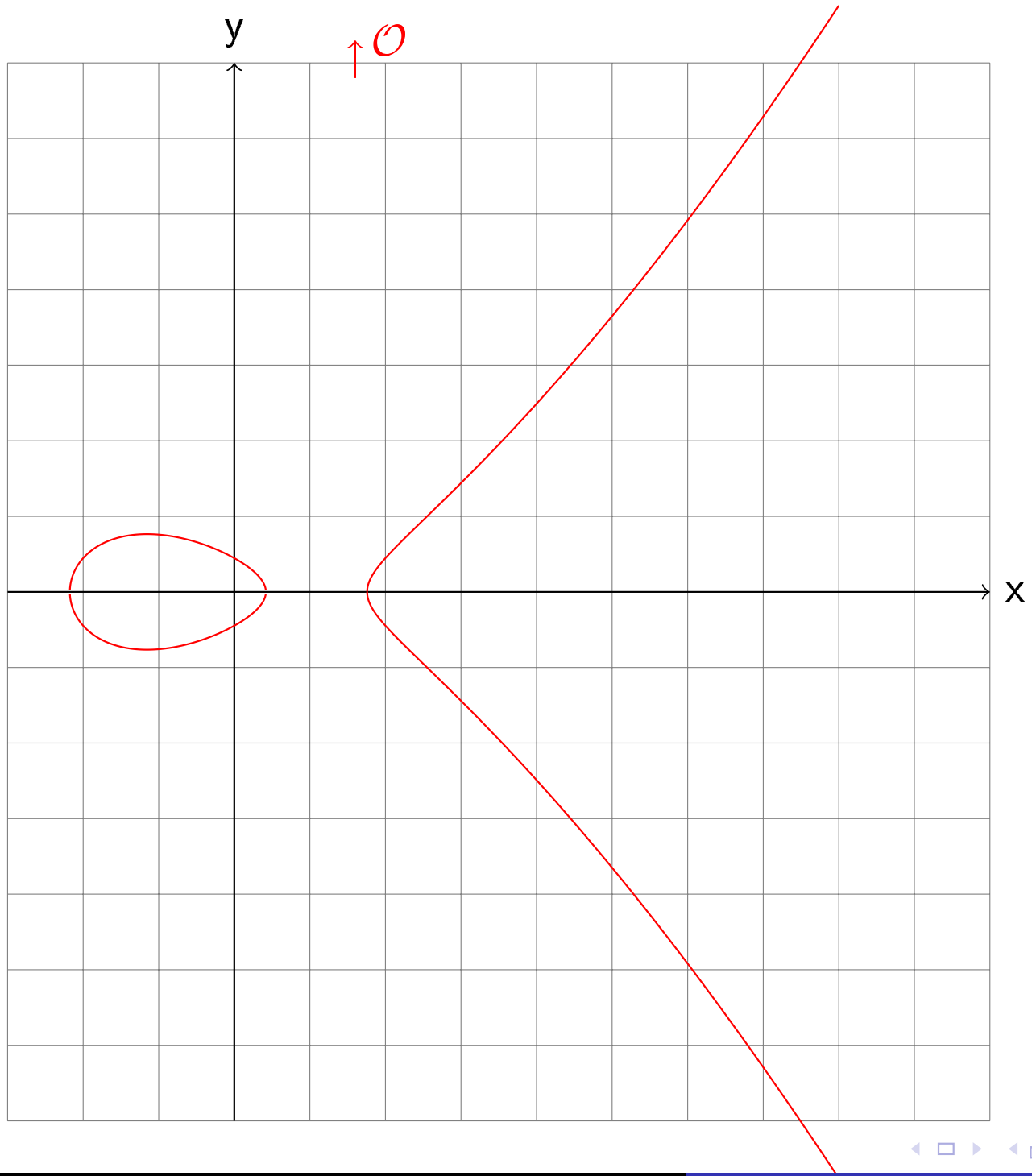
On ne peut donc pas, comme pour le cercle, faire une correspondance entre notre courbe et une droite : cette fois, la courbe n'est PAS une droite.

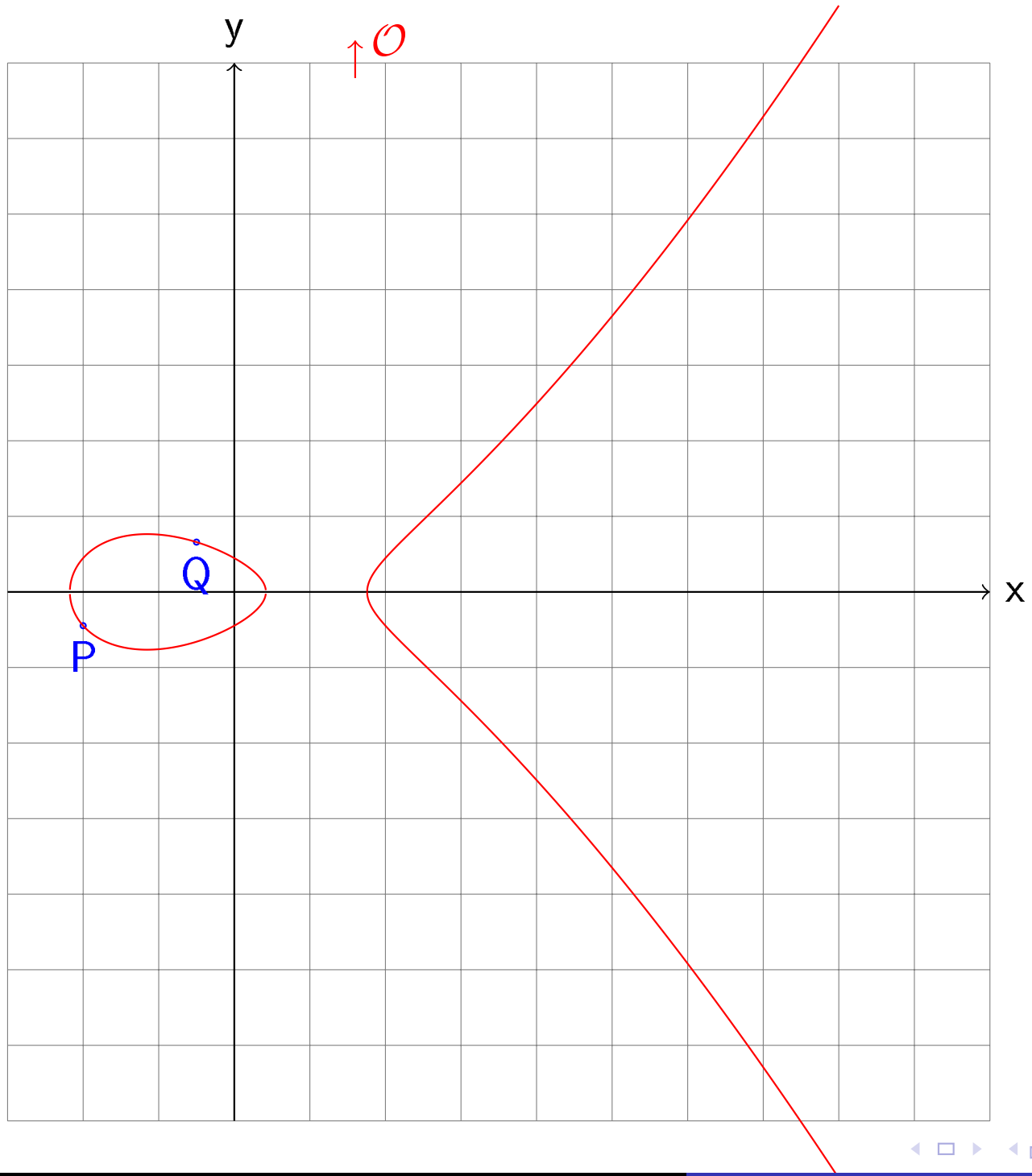
En revanche, si on prend deux points au hasard P et Q sur la courbe, alors la droite (PQ) coupe la courbe en trois points : P, Q, et un troisième point noté R'. On note enfin R le symmétrique de R' par rapport à l'axe horizontal.

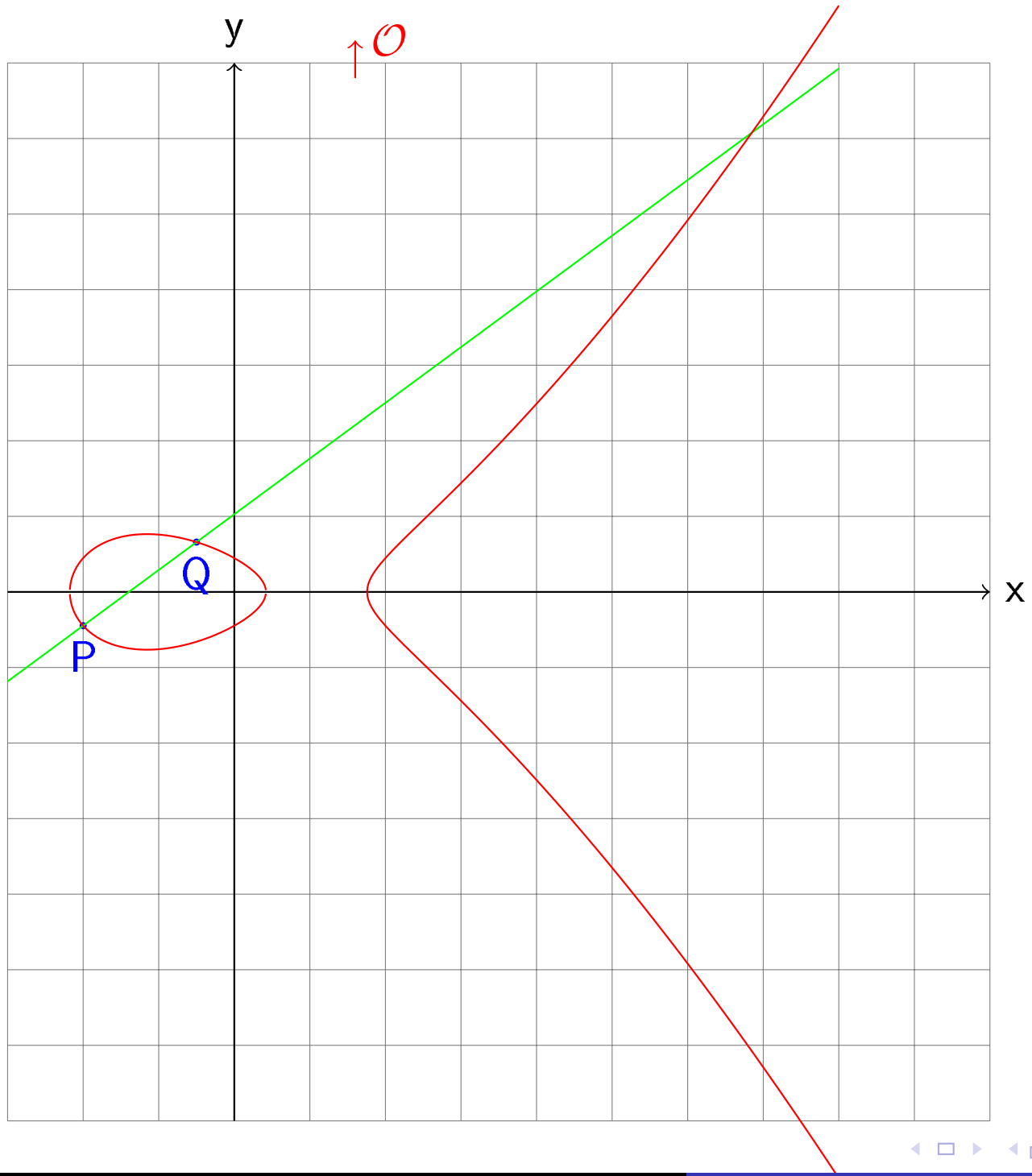
En revanche, si on prend deux points au hasard P et Q sur la courbe, alors la droite (PQ) coupe la courbe en trois points : P, Q, et un troisième point noté R'. On note enfin R le symmétrique de R' par rapport à l'axe horizontal.

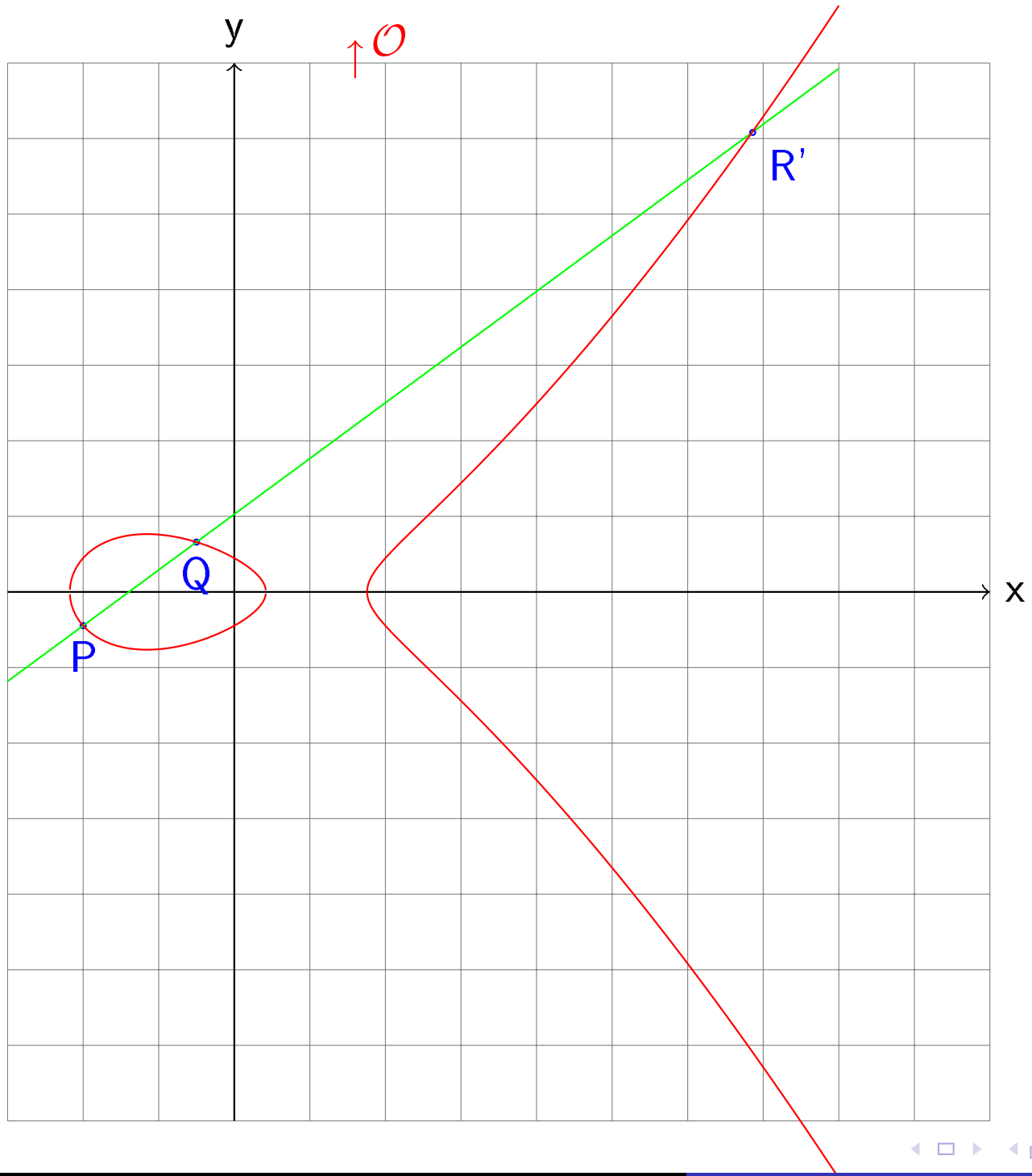
On décide de noter $R = P \oplus Q$, c'est-à-dire que l'on définit une façon d'additionner deux points de la courbe pour en obtenir un troisième.

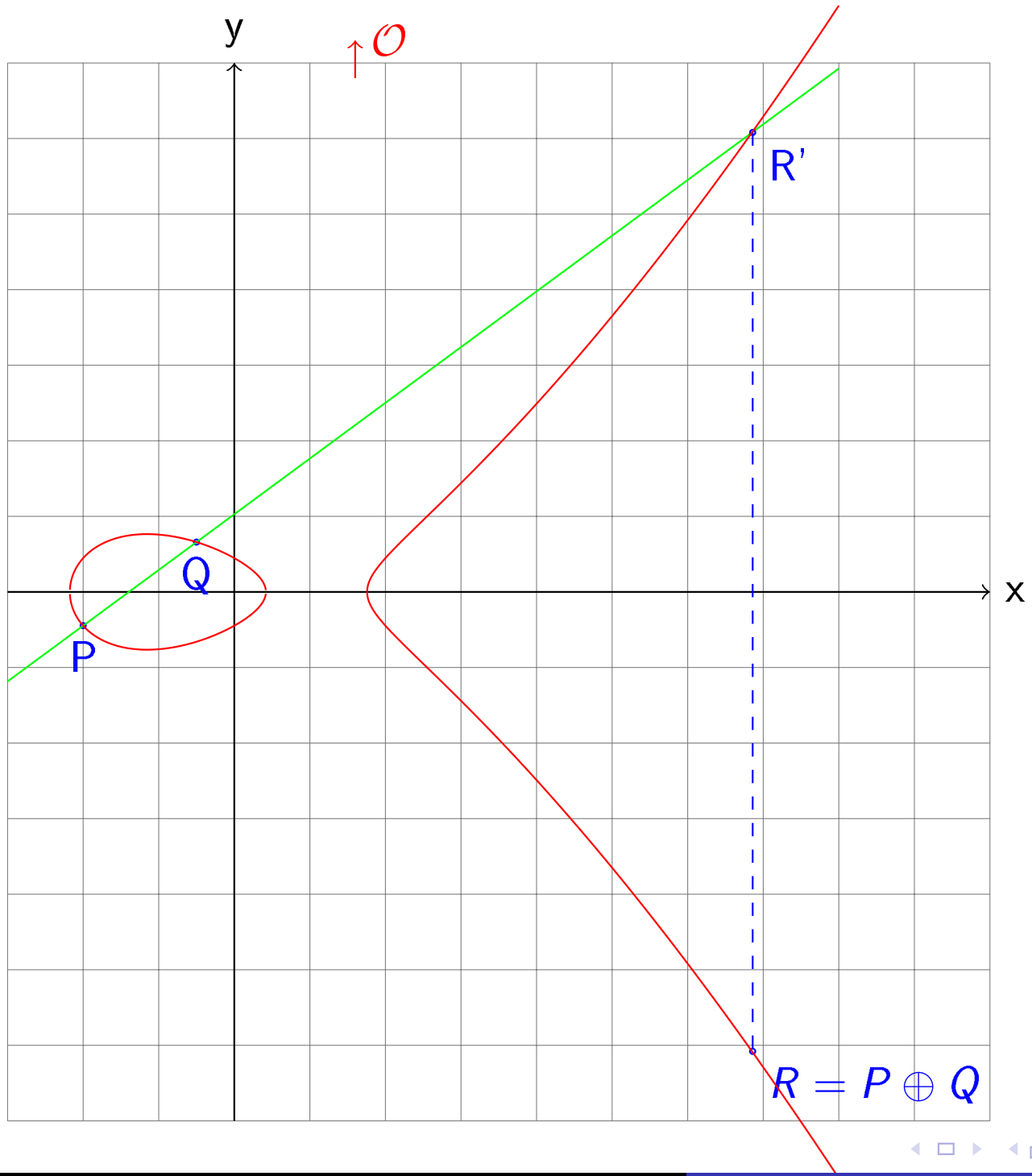

y
x


y
O
x


y
x
$\mathcal{O}$
Q
P


y
O
x
Q
P


y
O
R'
Q
P
x


y
$\mathcal{O}$
R'
Q
P
x
$R = P \oplus Q$

Addition des point de la courbe

On peut donc additionner d'autres objets que des nombres : ici, on additionne des points...

Addition des point de la courbe

On peut donc additionner d'autres objets que des nombres : ici, on additionne des points...

Cette "addition bizarre" a de très bonnes propriétés :

Addition des point de la courbe

On peut donc additionner d'autres objets que des nombres : ici, on additionne des points...

Cette "addition bizarre" a de très bonnes propriétés :

- Si P et Q sont à coordonnées rationnelles, alors $P \oplus Q$ est aussi à coordonnées rationnelles.

Addition des point de la courbe

On peut donc additionner d'autres objets que des nombres : ici, on additionne des points...

Cette "addition bizarre" a de très bonnes propriétés :

- Si P et Q sont à coordonnées rationnelles, alors $P \oplus Q$ est aussi à coordonnées rationnelles.
- $P \oplus Q = Q \oplus P$.

Addition des point de la courbe

On peut donc additionner d'autres objets que des nombres : ici, on additionne des points...

Cette "addition bizarre" a de très bonnes propriétés :

- Si P et Q sont à coordonnées rationnelles, alors $P \oplus Q$ est aussi à coordonnées rationnelles.
- $P \oplus Q = Q \oplus P$.
- $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$.

Addition des point de la courbe

On peut donc additionner d'autres objets que des nombres : ici, on additionne des points...

Cette "addition bizarre" a de très bonnes propriétés :

- Si P et Q sont à coordonnées rationnelles, alors $P \oplus Q$ est aussi à coordonnées rationnelles.
- $P \oplus Q = Q \oplus P$.
- $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$.
- si on rajoute un point (noté $\mathcal{O}$) "à l'infini" (voir dessin), alors $P \oplus \mathcal{O} = P$.

Addition des point de la courbe

On peut donc additionner d'autres objets que des nombres : ici, on additionne des points...

Cette "addition bizarre" a de très bonnes propriétés :

- Si P et Q sont à coordonnées rationnelles, alors $P \oplus Q$ est aussi à coordonnées rationnelles.
- $P \oplus Q = Q \oplus P$.
- $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$.
- si on rajoute un point (noté $\mathcal{O}$) "à l'infini" (voir dessin), alors $P \oplus \mathcal{O} = P$.
- pour tout point P de la courbe, on peut trouver un unique point P' tel que $P \oplus P' = \mathcal{O}$ (P' est le symmétrique de P par rapport à l'axe horizontal).

Ensemble des solutions rationnelles

Toutes ces propriétés font que l'addition $\oplus$ se comporte exactement comme l'addition habituelle des nombres. Donc on va pouvoir faire des calculs avec les points (plutôt qu'avec les nombres).

Ensemble des solutions rationnelles

Toutes ces propriétés font que l'addition $\oplus$ se comporte exactement comme l'addition habituelle des nombres. Donc on va pouvoir faire des calculs avec les points (plutôt qu'avec les nombres).

En utilisant cette façon d'additionner des points, les mathématiciens peuvent démontrer de très jolis résultats sur l'équation initiale.

Ensemble des solutions rationnelles

Toutes ces propriétés font que l'addition $\oplus$ se comporte exactement comme l'addition habituelle des nombres. Donc on va pouvoir faire des calculs avec les points (plutôt qu'avec les nombres).

En utilisant cette façon d'additionner des points, les mathématiciens peuvent démontrer de très jolis résultats sur l'équation initiale.

Théorème (Mordell-Weil 1928)

Toutes les solutions rationnelles sont obtenues en faisant des additions et des soustractions à partir d'un nombre fini de solutions. En quelque sorte, même s'il est infini, l'ensemble des solutions a une structure simple : à partir d'un nombre fini de solutions, on peut obtenir toutes les autres.

Ensemble des solutions rationnelles

Toutes ces propriétés font que l'addition $\oplus$ se comporte exactement comme l'addition habituelle des nombres. Donc on va pouvoir faire des calculs avec les points (plutôt qu'avec les nombres).

En utilisant cette façon d'additionner des points, les mathématiciens peuvent démontrer de très jolis résultats sur l'équation initiale.

Théorème (Mordell-Weil 1928)

Toutes les solutions rationnelles sont obtenues en faisant des additions et des soustractions à partir d'un nombre fini de solutions. En quelque sorte, même s'il est infini, l'ensemble des solutions a une structure simple : à partir d'un nombre fini de solutions, on peut obtenir toutes les autres.

Ensemble des solutions entières

On sait qu'il y a toujours moins de solutions entières que de solutions rationnelles. On peut dire mieux :

Ensemble des solutions entières

On sait qu'il y a toujours moins de solutions entières que de solutions rationnelles. On peut dire mieux :

Théorème (Siegel 1929)

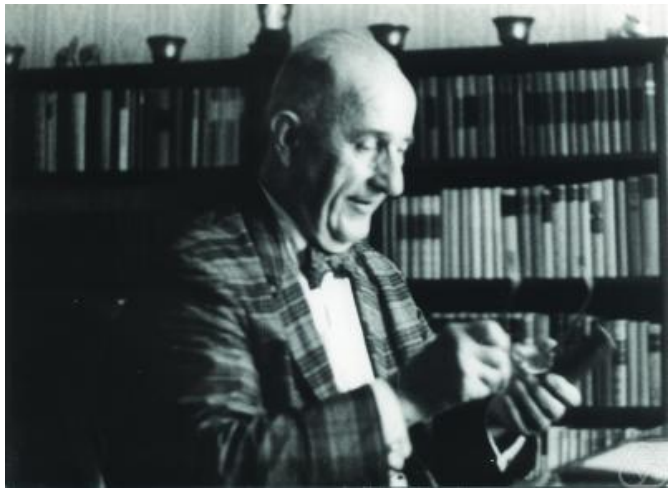
Il n'y a qu'un nombre fini de solutions entières, alors qu'il peut y avoir une infinité de solutions rationnelles.

Ensemble des solutions entières

On sait qu'il y a toujours moins de solutions entières que de solutions rationnelles. On peut dire mieux :

Théorème (Siegel 1929)

Il n'y a qu'un nombre fini de solutions entières, alors qu'il peut y avoir une infinité de solutions rationnelles.



Deux exemples

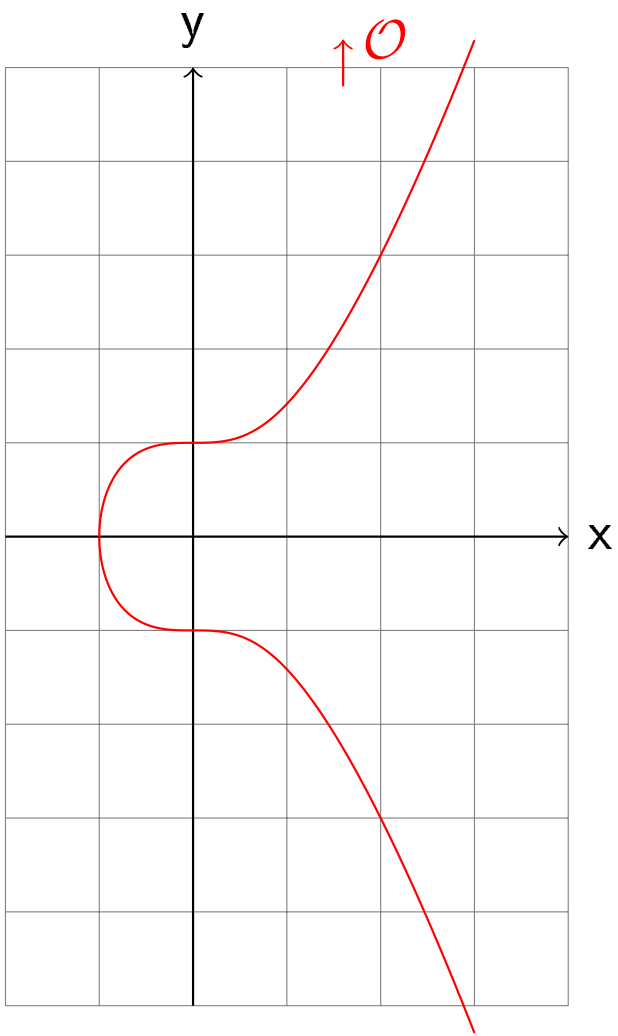
On s'intéresse à deux équations de degré 3 particulières.

Deux exemples

On s'intéresse à deux équations de degré 3 particulières.
Premier exemple : $y^2 = x^3 + 1$

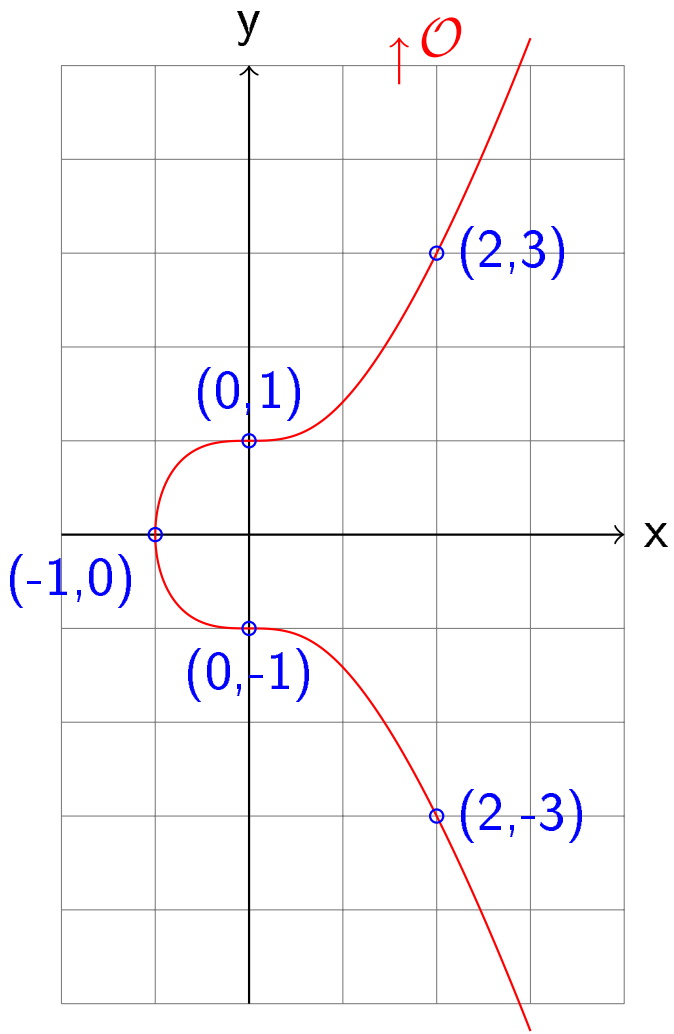
Deux exemples

On s'intéresse à deux équations de degré 3 particulières.
Premier exemple : $y^2 = x^3 + 1$



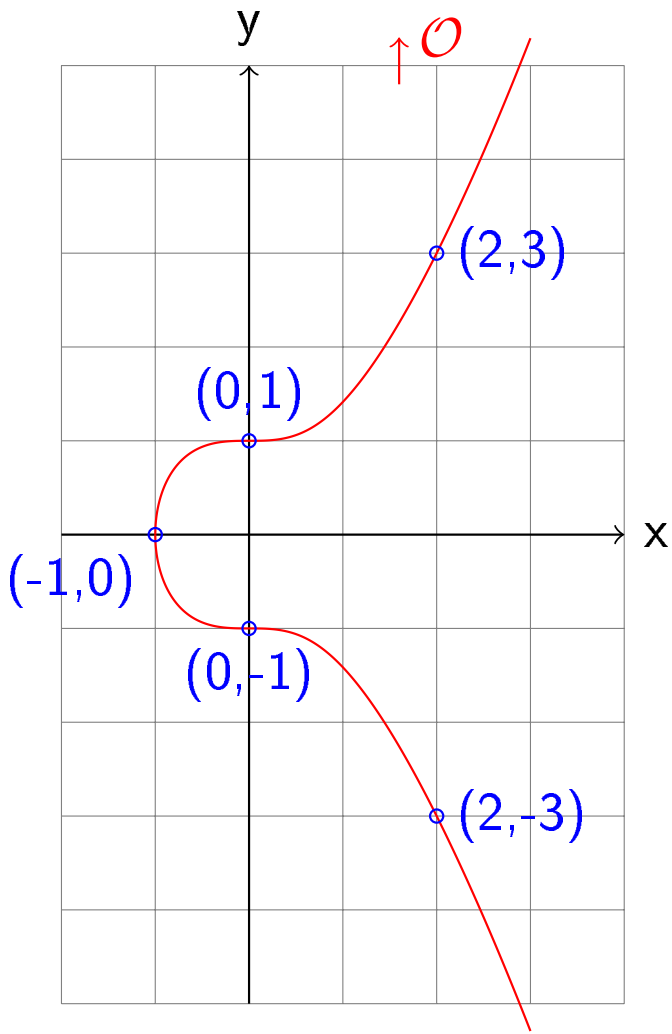
Deux exemples

On s'intéresse à deux équations de degré 3 particulières.
Premier exemple : $y^2 = x^3 + 1$



Deux exemples

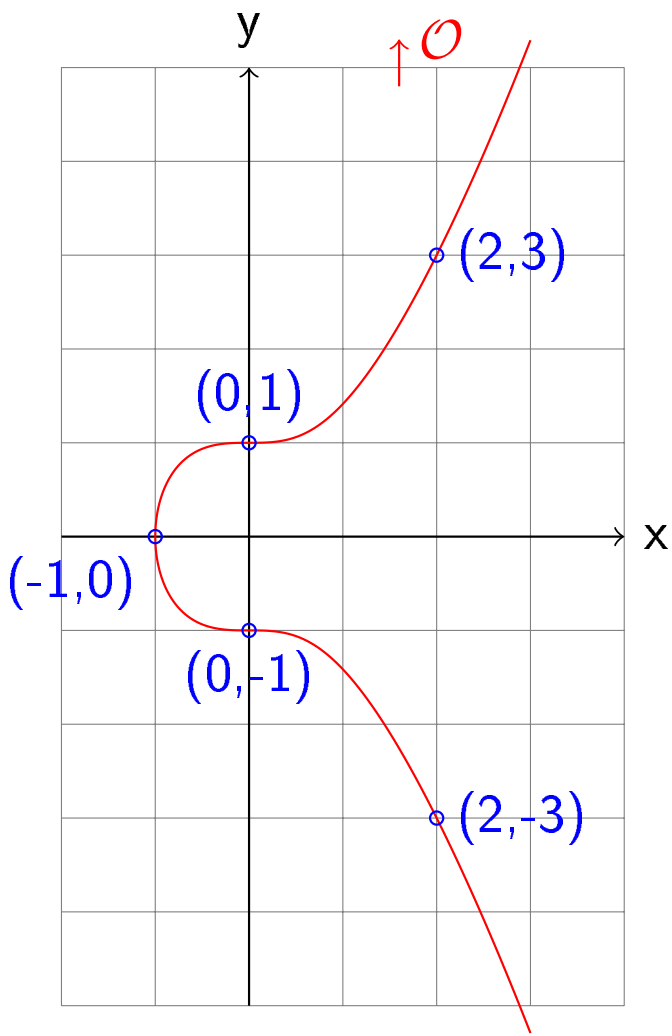
On s'intéresse à deux équations de degré 3 particulières.
Premier exemple : $y^2 = x^3 + 1$



Il n'y a qu'un nombre fini de points rationnels : les cinq points bleus de la figure.
On remarque que ces cinq points sont même à coordonnées entières.

Deux exemples

On s'intéresse à deux équations de degré 3 particulières.
Premier exemple : $y^2 = x^3 + 1$



Il n'y a qu'un nombre fini de points rationnels : les cinq points bleus de la figure.
On remarque que ces cinq points sont même à coordonnées entières.

Dans cet exemple, on a donc
cinq solutions rationnelles
cinq solutions entières.

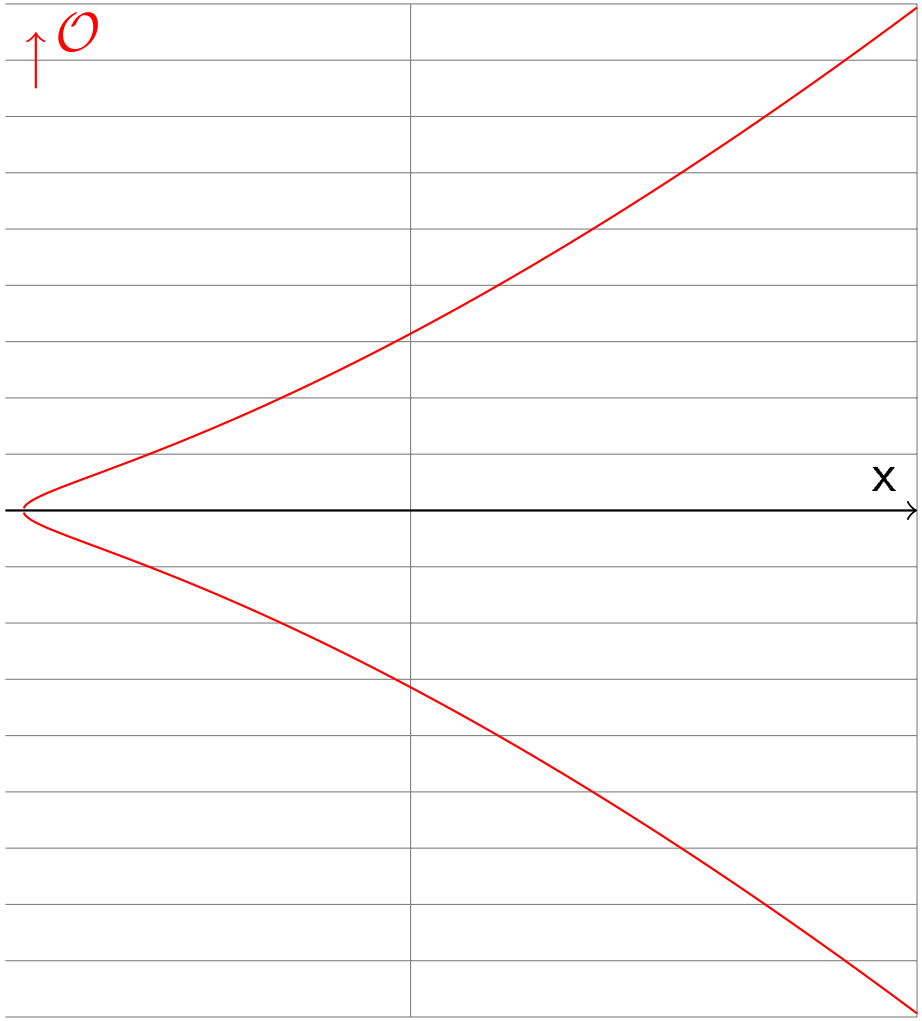
Deux exemples

Deux exemples

Second exemple : $y^2 = x^3 - 13$

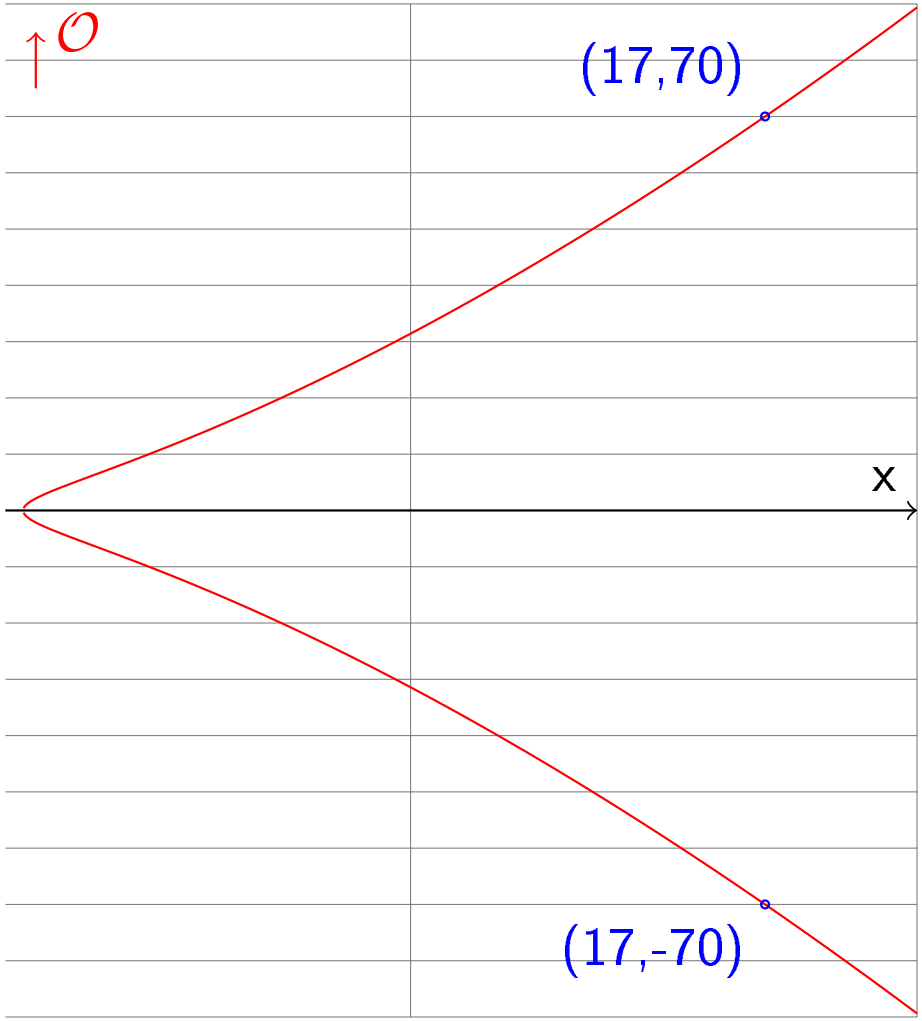
Deux exemples

Second exemple : $y^2 = x^3 - 13$



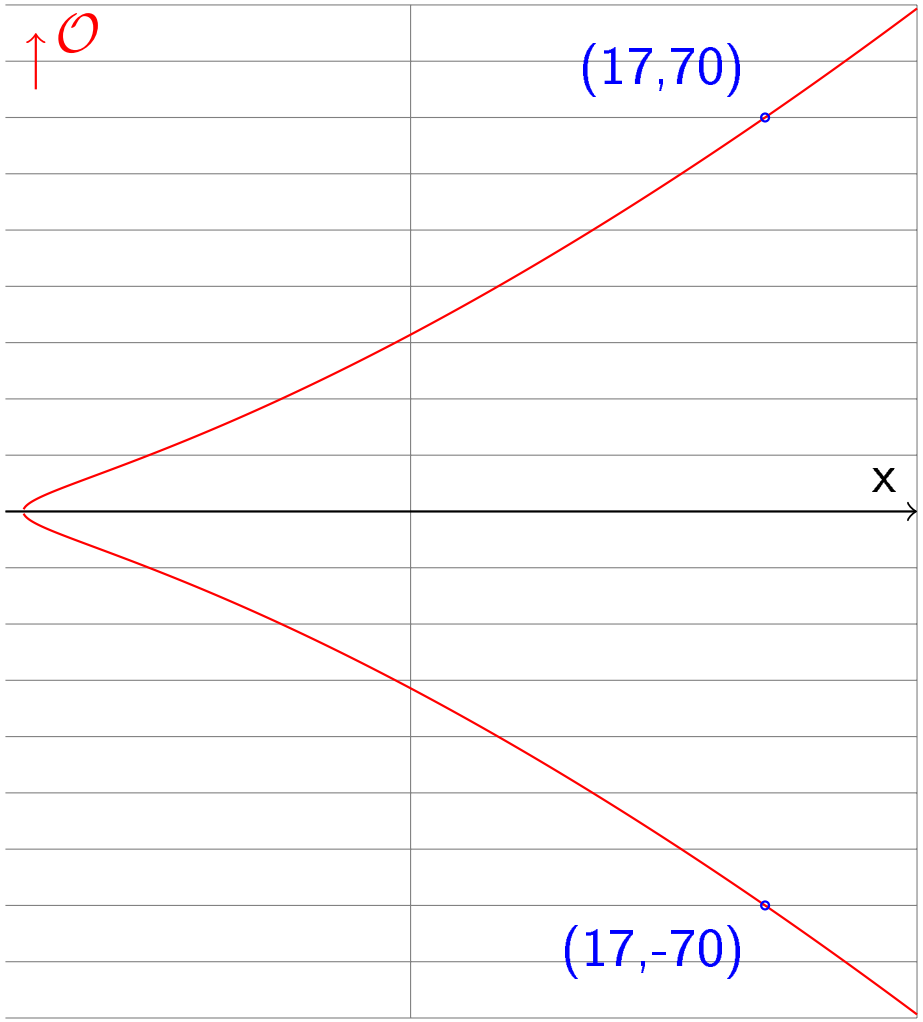
Deux exemples

Second exemple : $y^2 = x^3 - 13$



Deux exemples

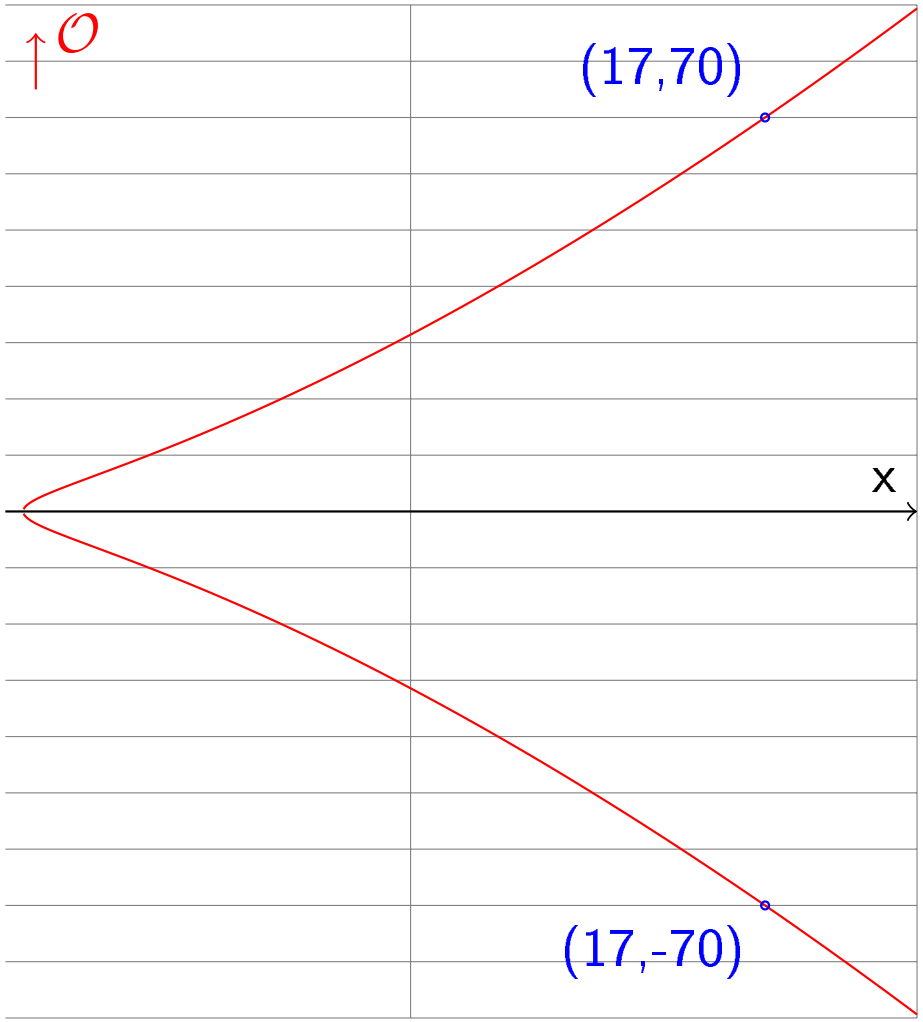
Second exemple : $y^2 = x^3 - 13$



Il y a une infinité de points rationnels, tous obtenus à partir des points bleus. Les deux points bleus sont les seuls points à coordonnées entières.

Deux exemples

Second exemple : $y^2 = x^3 - 13$

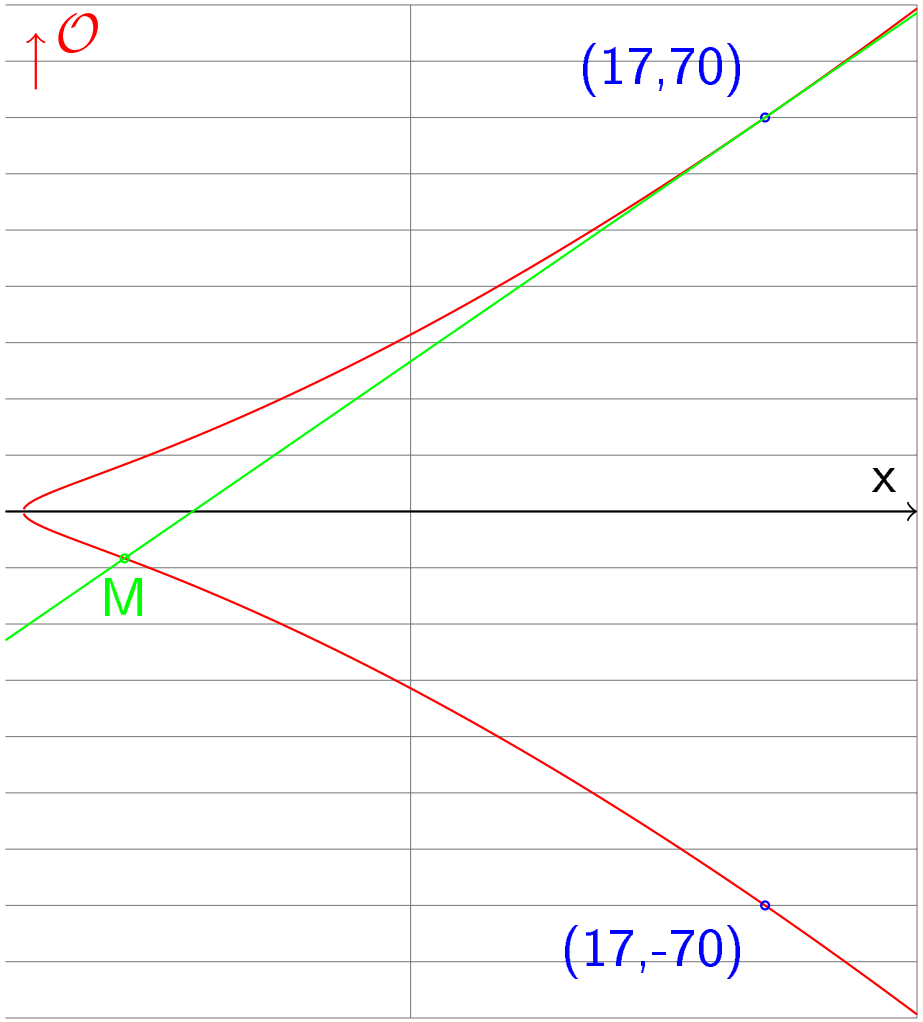


Il y a une infinité de points rationnels, tous obtenus à partir des points bleus. Les deux points bleus sont les seuls points à coordonnées entières.

Quand on additionne le point bleu avec lui-même, on trouve le point M à coordonnées rationnelles mais pas entières :
$M(\frac{85289}{19600}, -\frac{22858837}{2744000})$

Deux exemples

Second exemple : $y^2 = x^3 - 13$

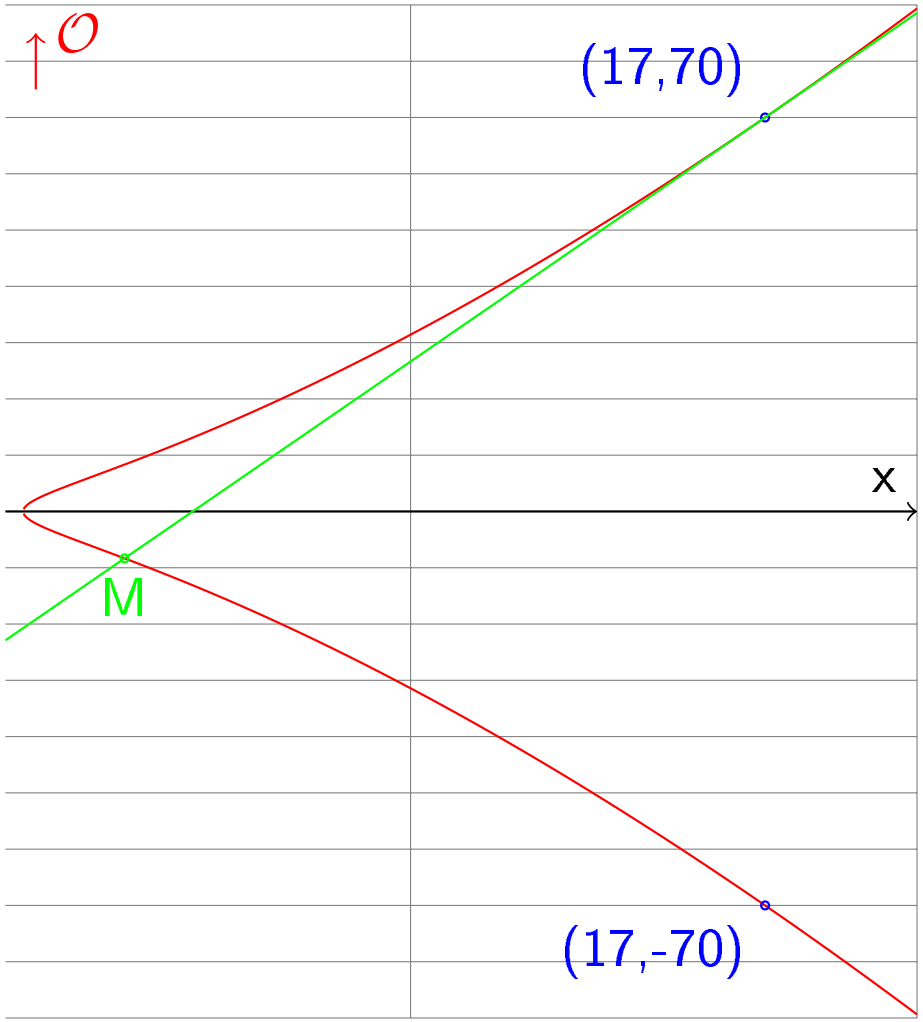


Il y a une infinité de points rationnels, tous obtenus à partir des points bleus. Les deux points bleus sont les seuls points à coordonnées entières.

Quand on additionne le point bleu avec lui-même, on trouve le point M à coordonnées rationnelles mais pas entières :
$\mathrm{M}(\frac{85289}{19600}, -\frac{22858837}{2744000})$

Deux exemples

Second exemple : $y^2 = x^3 - 13$



Il y a une infinité de points rationnels, tous obtenus à partir des points bleus.
Les deux points bleus sont les seuls points à coordonnées entières.

Quand on additionne le point bleu avec lui-même, on trouve le point M à coordonnées rationnelles mais pas entières :
$\mathrm{M}(\frac{85289}{19600}, -\frac{22858837}{2744000})$

Dans cet exemple, on a donc
une infinité de solutions rationnelles
deux solutions entières.

En degré supérieur

On a considéré pour le moment des équations de degré 1, 2 et 3. On peut résumer les résultats obtenus ainsi :

En degré supérieur

On a considéré pour le moment des équations de degré 1, 2 et 3. On peut résumer les résultats obtenus ainsi :

- en degré 1 et 2, soit on a aucune solution rationnelle, soit une infinité de solutions entières, et on dispose d'algorithmes pour décider dans quel cas on est et pour obtenir les formules pour toutes les solutions.

En degré supérieur

On a considéré pour le moment des équations de degré 1, 2 et 3. On peut résumer les résultats obtenus ainsi :

- en degré 1 et 2, soit on a aucune solution rationnelle, soit une infinité de solutions entières, et on dispose d'algorithmes pour décider dans quel cas on est et pour obtenir les formules pour toutes les solutions.
- en degré 3, on a soit aucune, soit un nombre fini, soit un nombre infini de solutions rationnelles. Dans tous les cas, on a un nombre fini de solutions entières.

En degré supérieur

On a considéré pour le moment des équations de degré 1, 2 et 3. On peut résumer les résultats obtenus ainsi :

- en degré 1 et 2, soit on a aucune solution rationnelle, soit une infinité de solutions entières, et on dispose d'algorithmes pour décider dans quel cas on est et pour obtenir les formules pour toutes les solutions.
- en degré 3, on a soit aucune, soit un nombre fini, soit un nombre infini de solutions rationnelles. Dans tous les cas, on a un nombre fini de solutions entières.

Que dire des équations de degré ≥ 4 ?

Degré ≥ 4

Ce problème est plus difficile encore que le degré 3. Mais on dispose du résultat suivant :

Degré ≥ 4

Ce problème est plus difficile encore que le degré 3. Mais on dispose du résultat suivant :

Théorème (Faltings 1983)

Pour les équations de degré ≥ 4, il n'y a qu'un nombre fini de solutions rationnelles.

Degré ≥ 4

Ce problème est plus difficile encore que le degré 3. Mais on dispose du résultat suivant :

Théorème (Faltings 1983)

Pour les équations de degré ≥ 4, il n'y a qu'un nombre fini de solutions rationnelles.

Degré ≥ 4

Ce problème est plus difficile encore que le degré 3. Mais on dispose du résultat suivant :

Théorème (Faltings 1983)

Pour les équations de degré ≥ 4, il n'y a qu'un nombre fini de solutions rationnelles.

En résumé, plus le degré est grand, moins l'équation a de solutions entières et rationnelles.

Équations à ≥ 3 inconnues

Pour le moment, on a regardé seulement des équations à deux inconnues (x et y), c'est-à-dire des courbes dans le plan.

Équations à ≥ 3 inconnues

Pour le moment, on a regardé seulement des équations à deux inconnues (x et y), c'est-à-dire des courbes dans le plan.

Cependant, beaucoup de problèmes mathématiques, physiques, biologiques, économiques, etc... font intervenir plus que deux inconnues !

Équations à ≥ 3 inconnues

Pour le moment, on a regardé seulement des équations à deux inconnues (x et y), c'est-à-dire des courbes dans le plan.

Cependant, beaucoup de problèmes mathématiques, physiques, biologiques, économiques, etc... font intervenir plus que deux inconnues !

Donc les mathématiciens s'intéressent beaucoup à des équations à 3 inconnues (ou plus).

Équations à ≥ 3 inconnues

Pour le moment, on a regardé seulement des équations à deux inconnues (x et y), c'est-à-dire des courbes dans le plan.

Cependant, beaucoup de problèmes mathématiques, physiques, biologiques, économiques, etc... font intervenir plus que deux inconnues !

Donc les mathématiciens s'intéressent beaucoup à des équations à 3 inconnues (ou plus).

Par exemple, les équations suivantes sont très utiles :

Équations à ≥ 3 inconnues

Pour le moment, on a regardé seulement des équations à deux inconnues (x et y), c'est-à-dire des courbes dans le plan.

Cependant, beaucoup de problèmes mathématiques, physiques, biologiques, économiques, etc... font intervenir plus que deux inconnues !

Donc les mathématiciens s'intéressent beaucoup à des équations à 3 inconnues (ou plus).

Par exemple, les équations suivantes sont très utiles :

$$x^2 + y^2 + z^2 = 3xyz$$

Équations à ≥ 3 inconnues

Pour le moment, on a regardé seulement des équations à deux inconnues (x et y), c'est-à-dire des courbes dans le plan.

Cependant, beaucoup de problèmes mathématiques, physiques, biologiques, économiques, etc... font intervenir plus que deux inconnues !

Donc les mathématiciens s'intéressent beaucoup à des équations à 3 inconnues (ou plus).

Par exemple, les équations suivantes sont très utiles :

$$x^2 + y^2 + z^2 = 3xyz$$

$$x^p + y^q = z^r$$

Équations à ≥ 3 inconnues

Pour le moment, on a regardé seulement des équations à deux inconnues (x et y), c'est-à-dire des courbes dans le plan.

Cependant, beaucoup de problèmes mathématiques, physiques, biologiques, économiques, etc... font intervenir plus que deux inconnues !

Donc les mathématiciens s'intéressent beaucoup à des équations à 3 inconnues (ou plus).

Par exemple, les équations suivantes sont très utiles :

$$x^2 + y^2 + z^2 = 3xyz$$

$$x^p + y^q = z^r$$

Quels sont les entiers n qui sont sommes de k-puissances r-ièmes :

$$x_1^r + x_2^r + \cdots + x_k^r = n\,?$$

Équations à ≥ 3 inconnues

En général, on sait très peu de choses sur ces équations.

.

Équations à ≥ 3 inconnues

En général, on sait très peu de choses sur ces équations.

1. Si le degré de l'équation est ≤ 2 (même avec beaucoup d'inconnues), alors on a des algorithmes pour savoir si l'équation a des solutions ou non, puis pour déterminer ces solutions.

.

Équations à ≥ 3 inconnues

En général, on sait très peu de choses sur ces équations.

1. Si le degré de l'équation est ≤ 2 (même avec beaucoup d'inconnues), alors on a des algorithmes pour savoir si l'équation a des solutions ou non, puis pour déterminer ces solutions.
2. Si on a une ou deux inconnues seulement (même pour des équations de grand degré), alors on sait beaucoup de choses (comme on l'a vu jusqu'ici) car la géométrie des courbes dans le plan est "assez simple".

Équations à ≥ 3 inconnues

En général, on sait très peu de choses sur ces équations.

1. Si le degré de l'équation est ≤ 2 (même avec beaucoup d'inconnues), alors on a des algorithmes pour savoir si l'équation a des solutions ou non, puis pour déterminer ces solutions.
2. Si on a une ou deux inconnues seulement (même pour des équations de grand degré), alors on sait beaucoup de choses (comme on l'a vu jusqu'ici) car la géométrie des courbes dans le plan est "assez simple".
3. En revanche, dès que l'on a au moins trois inconnues et une équation de degré ≥ 3, alors c'est très difficile et on sait très peu de choses...

Géométrie en dimension ≥ 3

La résolution des équations est plus difficile quand on a ≥ 3 inconnues parce que la géométrie est plus compliquée.

En effet,

Géométrie en dimension ≥ 3

La résolution des équations est plus difficile quand on a ≥ 3 inconnues parce que la géométrie est plus compliquée.

En effet,

1. une équation à deux inconnues définit une courbe dans le plan.

Géométrie en dimension ≥ 3

La résolution des équations est plus difficile quand on a ≥ 3 inconnues parce que la géométrie est plus compliquée.

En effet,

1. une équation à deux inconnues définit une courbe dans le plan.
2. une équation à trois inconnues définit une surface dans l'espace.

Géométrie en dimension ≥ 3

La résolution des équations est plus difficile quand on a ≥ 3 inconnues parce que la géométrie est plus compliquée.

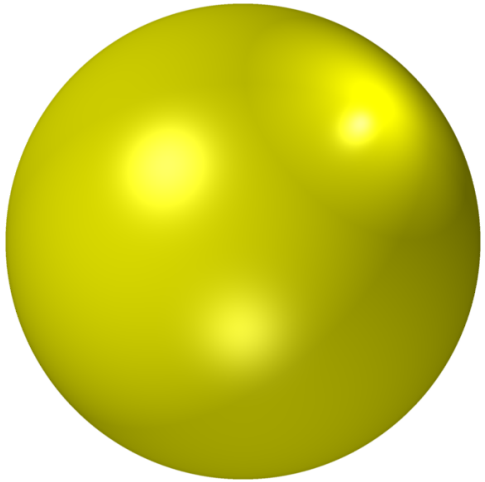
En effet,

1. une équation à deux inconnues définit une courbe dans le plan.
2. une équation à trois inconnues définit une surface dans l'espace.
3. une équation à quatre inconnues défini un objet de dimension 3 dans un espace de dimension 4...

Voici quelques exemples de surfaces dans un espace de dimension 3 définies par des équations à 3 inconnues :

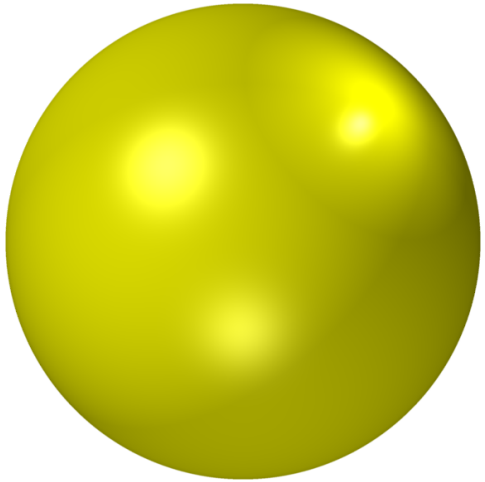
Voici quelques exemples de surfaces dans un espace de dimension 3 définies par des équations à 3 inconnues :

- $x^2 + y^2 + z^2 = 1$

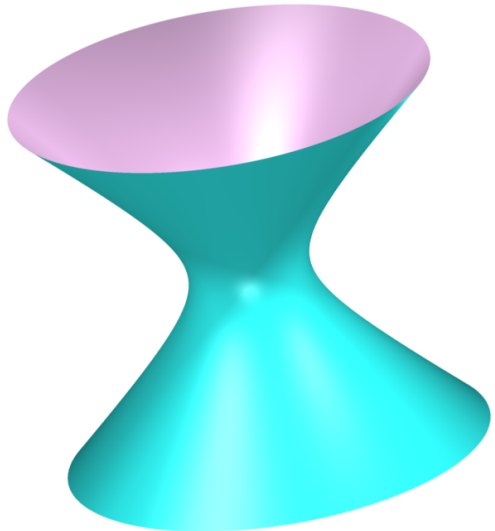


Voici quelques exemples de surfaces dans un espace de dimension 3 définies par des équations à 3 inconnues :

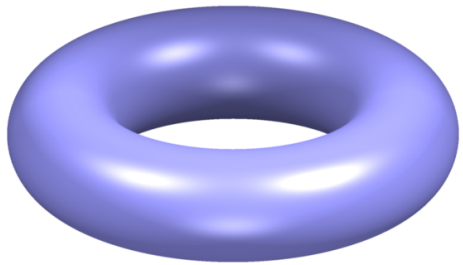
- $x^2 + y^2 + z^2 = 1$



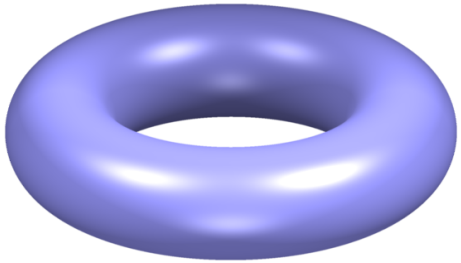
- $x^2 + y^2 - z^2 = 1$



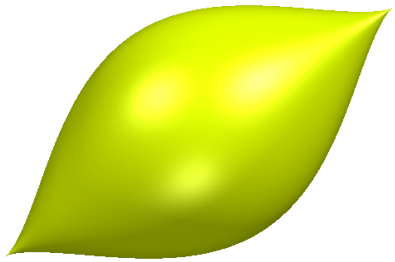
- $(x^2 + y^2 + z^2 + 2)^2 - 9(x^2 + y^2) = 0$



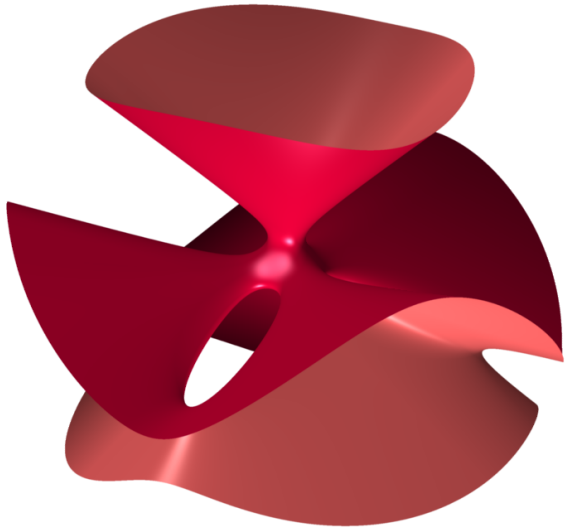
- $(x^2 + y^2 + z^2 + 2)^2 - 9(x^2 + y^2) = 0$



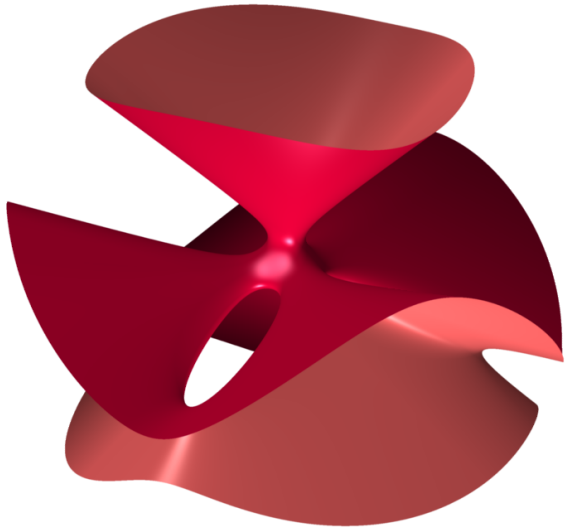
- $1.2x^2 + 1.2z^2 - 5(y + 0.5)^3(0.5 - y)^3 = 0$



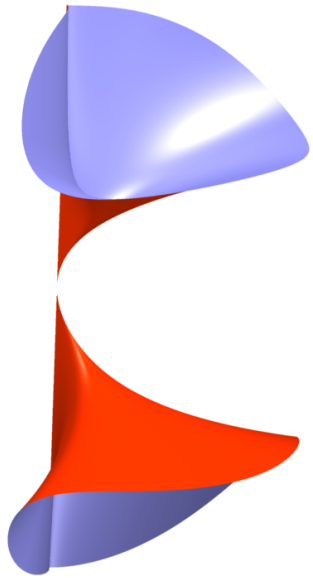
- $x^3 + y^3 + z^3 + 1 - 0.5(x + y + z + 1)^3 = 0$



- $x^3 + y^3 + z^3 + 1 - 0.5(x + y + z + 1)^3 = 0$



- $x^2 + y^4 + y^3 z^2 = 0$



- $(x^2 + \frac{9}{4}y^2 + z^2 - 1)^3 - x^2z^3 - \frac{9}{80}y^2z^3 = 0$

Un résultat négatif

En général, en dimension ≥ 3, la résolution des équations arithmétiques est donc un problème très compliqué. On peut même montrer le résultat suivant :

Un résultat négatif

En général, en dimension ≥ 3, la résolution des équations arithmétiques est donc un problème très compliqué. On peut même montrer le résultat suivant :

Théorème (Davis-Matiyasevich-Putnam-Robinson 1970)

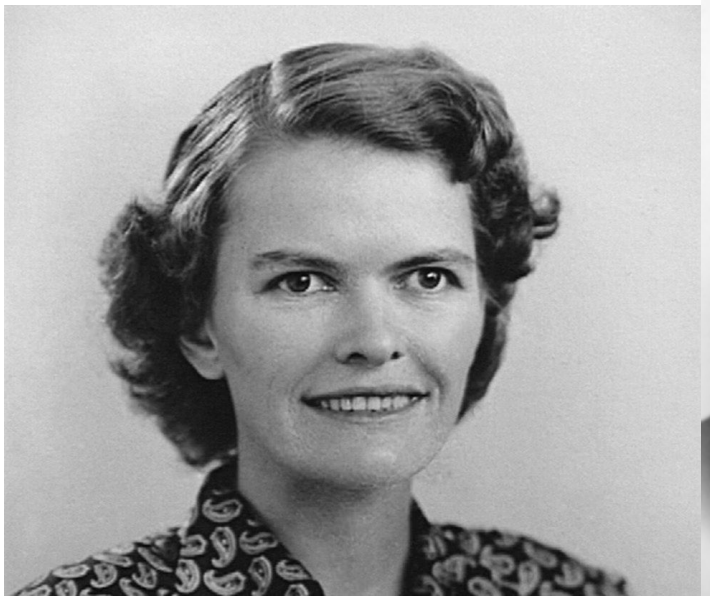
Il est impossible de trouver un algorithme qui puisse résoudre toutes les équations arithmétiques.

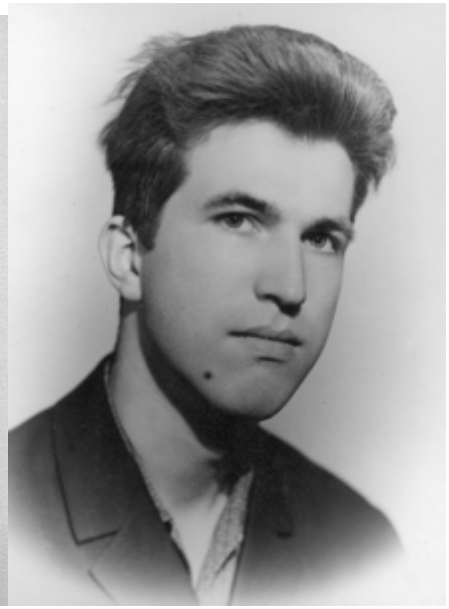
Un résultat négatif

En général, en dimension ≥ 3, la résolution des équations arithmétiques est donc un problème très compliqué. On peut même montrer le résultat suivant :

Théorème (Davis-Matiyasevich-Putnam-Robinson 1970)

Il est impossible de trouver un algorithme qui puisse résoudre toutes les équations arithmétiques.



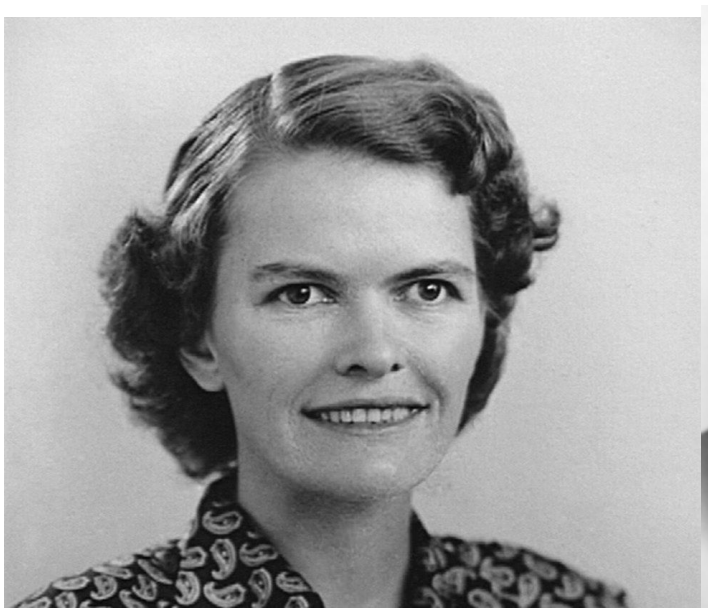


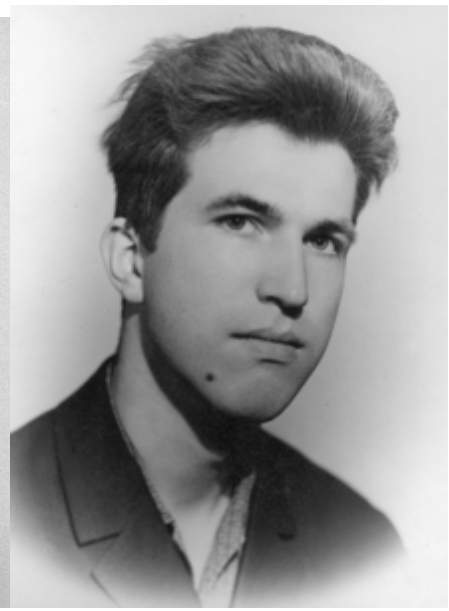
Un résultat négatif

En général, en dimension ≥ 3, la résolution des équations arithmétiques est donc un problème très compliqué. On peut même montrer le résultat suivant :

Théorème (Davis-Matiyasevich-Putnam-Robinson 1970)

Il est impossible de trouver un algorithme qui puisse résoudre toutes les équations arithmétiques.





Heureusement pour les mathématiciens, on peut donc démontrer qu'un ordinateur ne pourra pas vraiment nous remplacer...

Maintenant, la question rituelle...

Maintenant, un certain nombre d'entre vous doit se demander :

Maintenant, la question rituelle...

Maintenant, un certain nombre d'entre vous doit se demander :

C'est bien beau, tout ça, mais À QUOI ÇA SERT ??

Maintenant, la question rituelle...

Maintenant, un certain nombre d'entre vous doit se demander :

C'est bien beau, tout ça, mais À QUOI ÇA SERT ??

1. Première réponse : ce sont des questions simples, très naturelles, que les hommes se posent depuis des milliers d'années (lemme chinois, problème de Pythagore, théorème de Fermat, etc...) : on ne peut pas s'empêcher d'y réfléchir.

Maintenant, la question rituelle...

Maintenant, un certain nombre d'entre vous doit se demander :

C'est bien beau, tout ça, mais À QUOI ÇA SERT ??

1. Première réponse : ce sont des questions simples, très naturelles, que les hommes se posent depuis des milliers d'années (lemme chinois, problème de Pythagore, théorème de Fermat, etc...) : on ne peut pas s'empêcher d'y réfléchir.
2. Deuxième réponse : ce sont des mathématiques et des raisonnements très jolis, et c'est très plaisant, intéressant, amusant même, de travailler sur ces questions.

Maintenant, la question rituelle...

Maintenant, un certain nombre d'entre vous doit se demander :

C'est bien beau, tout ça, mais À QUOI ÇA SERT ??

1. Première réponse : ce sont des questions simples, très naturelles, que les hommes se posent depuis des milliers d'années (lemme chinois, problème de Pythagore, théorème de Fermat, etc...) : on ne peut pas s'empêcher d'y réfléchir.
2. Deuxième réponse : ce sont des mathématiques et des raisonnements très jolis, et c'est très plaisant, intéressant, amusant même, de travailler sur ces questions.
3. Troisième réponse, plus concrète et plus terre à terre : beaucoup d'applications, par exemple en cryptographie.

Applications en cryptographie

Les courbes elliptiques (équations de degré 3) et leurs points rationnels sont utilisés dans vos téléphones portables, smartphones, dans vos ordinateurs, dans vos cartes bancaires, etc... pour crypter, protéger, transmettre vos données.

Applications en cryptographie

Les courbes elliptiques (équations de degré 3) et leurs points rationnels sont utilisés dans vos téléphones portables, smartphones, dans vos ordinateurs, dans vos cartes bancaires, etc... pour crypter, protéger, transmettre vos données.

En général, Alice et Bob souhaite communiquer sans se faire espionner, et pour cela, ils utilisent une clé pour coder leurs messages. Par exemple : on choisit un nombre entier entre 0 et 25 (la clé) et on décide de décaler les lettres de cet entier fixé.

Applications en cryptographie

Les courbes elliptiques (équations de degré 3) et leurs points rationnels sont utilisés dans vos téléphones portables, smartphones, dans vos ordinateurs, dans vos cartes bancaires, etc... pour crypter, protéger, transmettre vos données.

En général, Alice et Bob souhaite communiquer sans se faire espionner, et pour cela, ils utilisent une clé pour coder leurs messages. Par exemple : on choisit un nombre entier entre 0 et 25 (la clé) et on décide de décaler les lettres de cet entier fixé.

Problème : comment choisir la clé et la partager (entre Alice et Bob) sans que personne d'autre ne la connaisse ?

Comment fabriquer une clé secrète partagée ?

Alice et Bob cherchent à fabriquer une clé secrète qu'ils seront les seuls à connaître.

Comment fabriquer une clé secrète partagée ?

Alice et Bob cherchent à fabriquer une clé secrète qu'ils seront les seuls à connaître.
Voici le principe simplifié.

Comment fabriquer une clé secrète partagée ?

Alice et Bob cherchent à fabriquer une clé secrète qu'ils seront les seuls à connaître.
Voici le principe simplifié.

1. Ils choisissent une courbe elliptique E (une équation de degré 3) et un point P sur cette courbe E (une solution de cette équation).

Comment fabriquer une clé secrète partagée ?

Alice et Bob cherchent à fabriquer une clé secrète qu'ils seront les seuls à connaître.
Voici le principe simplifié.

1. Ils choisissent une courbe elliptique E (une équation de degré 3) et un point P sur cette courbe E (une solution de cette équation).
2. Alice choisit un nombre secret a et Bob un nombre secret b ($a, b \in \mathbb{N}$).

Comment fabriquer une clé secrète partagée ?

Alice et Bob cherchent à fabriquer une clé secrète qu'ils seront les seuls à connaître.
Voici le principe simplifié.

1. Ils choisissent une courbe elliptique E (une équation de degré 3) et un point P sur cette courbe E (une solution de cette équation).
2. Alice choisit un nombre secret a et Bob un nombre secret b ($a, b \in \mathbb{N}$).
3. Alice calcule le point $Q := aP = P + \cdots + P$ de E et l'envoie à Bob. Dans le même temps, Bob calcule $R := bP$ et l'envoie à Alice.

Comment fabriquer une clé secrète partagée ?

Alice et Bob cherchent à fabriquer une clé secrète qu'ils seront les seuls à connaître.
Voici le principe simplifié.

1. Ils choisissent une courbe elliptique E (une équation de degré 3) et un point P sur cette courbe E (une solution de cette équation).
2. Alice choisit un nombre secret a et Bob un nombre secret b ($a, b \in \mathbb{N}$).
3. Alice calcule le point $Q := aP = P + \cdots + P$ de E et l'envoie à Bob. Dans le même temps, Bob calcule $R := bP$ et l'envoie à Alice.
4. Alice calcule le point $S := aQ = (ab)P$ de E, et Bob calcule $S' = bR = (ba)P = S$.

Comment fabriquer une clé secrète partagée ?

Alice et Bob cherchent à fabriquer une clé secrète qu'ils seront les seuls à connaître.
Voici le principe simplifié.

1. Ils choisissent une courbe elliptique E (une équation de degré 3) et un point P sur cette courbe E (une solution de cette équation).
2. Alice choisit un nombre secret a et Bob un nombre secret b ($a, b \in \mathbb{N}$).
3. Alice calcule le point $Q := aP = P + \cdots + P$ de E et l'envoie à Bob. Dans le même temps, Bob calcule $R := bP$ et l'envoie à Alice.
4. Alice calcule le point $S := aQ = (ab)P$ de E, et Bob calcule $S' = bR = (ba)P = S$.
5. Alice et Bob utilisent alors les coordonnées du point S pour fabriquer leur clé secrète : par exemple, ils décident que la clé secrète est l'abscisse du point S.

Comment fabriquer une clé secrète partagée ?

Maintenant qu'ils ont construit leur clé secrète, Alice et Bob peuvent communiquer en utilisant cette clé sans se faire espionner.

Comment fabriquer une clé secrète partagée ?

Maintenant qu'ils ont construit leur clé secrète, Alice et Bob peuvent communiquer en utilisant cette clé sans se faire espionner.

Par exemple, si la clé est 3142 et si Alice veut envoyer le mot 1234 à Bob :

Comment fabriquer une clé secrète partagée ?

Maintenant qu'ils ont construit leur clé secrète, Alice et Bob peuvent communiquer en utilisant cette clé sans se faire espionner.

Par exemple, si la clé est 3142 et si Alice veut envoyer le mot 1234 à Bob :

1. Alice décale les lettres de son mot en ajoutant les chiffres de sa clé : 1234 devient 4376.

Comment fabriquer une clé secrète partagée ?

Maintenant qu'ils ont construit leur clé secrète, Alice et Bob peuvent communiquer en utilisant cette clé sans se faire espionner.

Par exemple, si la clé est 3142 et si Alice veut envoyer le mot 1234 à Bob :

1. Alice décale les lettres de son mot en ajoutant les chiffres de sa clé : 1234 devient 4376.
2. Alice envoie 4376, et Bob peut retrouver le message initial 1234 en enlevant les chiffres de la clé.

Comment fabriquer une clé secrète partagée ?

Maintenant qu'ils ont construit leur clé secrète, Alice et Bob peuvent communiquer en utilisant cette clé sans se faire espionner.

Par exemple, si la clé est 3142 et si Alice veut envoyer le mot 1234 à Bob :

1. Alice décale les lettres de son mot en ajoutant les chiffres de sa clé : 1234 devient 4376.
2. Alice envoie 4376, et Bob peut retrouver le message initial 1234 en enlevant les chiffres de la clé.
3. On peut démontrer que l'espion Charles ne peut pas deviner la clé secrète s'il connaît seulement la courbe E et les points P, Q, R, mais pas la clé.

Comment fabriquer une clé secrète partagée ?

Maintenant qu'ils ont construit leur clé secrète, Alice et Bob peuvent communiquer en utilisant cette clé sans se faire espionner.

Par exemple, si la clé est 3142 et si Alice veut envoyer le mot 1234 à Bob :

1. Alice décale les lettres de son mot en ajoutant les chiffres de sa clé : 1234 devient 4376.
2. Alice envoie 4376, et Bob peut retrouver le message initial 1234 en enlevant les chiffres de la clé.
3. On peut démontrer que l'espion Charles ne peut pas deviner la clé secrète s'il connaît seulement la courbe E et les points P, Q, R, mais pas la clé.
4. Le point crucial est qu'en général, si on connaît seulement E, P, aP, bP, on ne peut pas calculer rapidement $(ab)P$ et donc en déduire la clé.

Mais comment fait la NSA ?

On peut donc démontrer mathématiquement qu'il est impossible d'espionner des conversations qui utilisent cette méthode de codage.

Mais comment fait la NSA ?

On peut donc démontrer mathématiquement qu'il est impossible d'espionner des conversations qui utilisent cette méthode de codage.

Mais comment expliquer ceci ?

Mais comment fait la NSA ?

On peut donc démontrer mathématiquement qu'il est impossible d'espionner des conversations qui utilisent cette méthode de codage.

Mais comment expliquer ceci ?


Le Monde

LE MONDE DES LIVRES

LE LOUP ARRIVE EN PLAINE, ET SÈME LA PANIQUE

UNE « BIO » REMARQUABLE SUR LE GÉNÉRAL DUMAS, CE MULÂTRE

Espionnage américain : le coup de colère d'Angela Merkel

Les Etats-Unis, suspectés d'espionner les chefs d'Etat, sont en position d'accusés avant le sommet européen


FIGARO

FISCALITÉ

PEL, PEA, ASSURANCE-VIE : LES ÉPARGNANTS PIÉGÉS PAR LA RÉTROACTIVITÉ DE L'IMPÔT

Espionnage : la colère des Européens contre Obama

Les révélations sur la surveillance américaine du téléphone portable d'Angela Merkel dominent le sommet européen. Critiquée, la Maison-Blanche refuse de s'expliquer en détail.


whistleblower

I can't allow the US government to destroy privacy and basic liberties

theguardian

PRISM

The Washington Post

who leaked NSA secrets steps forward

A trading probe with 400 insiders

Mais comment fait la NSA ?

Dans un article récent, Thomas C. Hales (mathématicien américain) explique comment la NSA aurait réussi à contourner les méthodes de cryptographie que l'on a vues pour réussir à lire vos emails et à écouter vos conversations téléphoniques.

Mais comment fait la NSA ?

Dans un article récent, Thomas C. Hales (mathématicien américain) explique comment la NSA aurait réussi à contourner les méthodes de cryptographie que l'on a vues pour réussir à lire vos emails et à écouter vos conversations téléphoniques.

Mais comment fait la NSA ?

The NSA back door to NIST

SEPTEMBER 25, 2013

THALES

LEAVE A COMMENT

Thomas C. Hales (University of Pittsburgh)

(This article will be published in the *Notices of the American Mathematical Society*.)

Use once. Die once. — activist saying about insecure communication

This article gives a brief mathematical description of the NIST standard for cryptographically secure pseudo-random number generation by elliptic curves, the back door to the algorithm discovered by Ferguson and Shumow, and finally the design of the back door based on the Diffie-Hellman key exchange algorithm.

NIST (the National Institute for Standards and Technology) of the U.S. Department of Commerce derives its mandate from the U.S. Constitution, through the congressional power to "fix the standard of weights and measures." In brief, NIST establishes the basic standards of science and commerce. Whatever NIST says about cryptography becomes implemented in cryptographic applications throughout U.S. government agencies. Its influence leads to the widespread use of its standards in industry and the broad adoption of its standards internationally.

Through the Snowden disclosures, the NIST standard for pseudo-random number generation has fallen into disrepute. Here I describe the back door to the NIST standard for pseudo-random number generation in elementary

Follow

Mais comment fait la NSA ? (version simplifiée)

Mais comment fait la NSA ? (version simplifiée)

1. Le NIST (National Institute on Standards and Technology) fournit à une entreprise d'informatique A les données suivantes :

Mais comment fait la NSA ? (version simplifiée)

1. Le NIST (National Institute on Standards and Technology) fournit à une entreprise d'informatique A les données suivantes : une courbe elliptique E (donnée par une équation), et des points P et Q sur E, où Q est de la forme aP.

Mais comment fait la NSA ? (version simplifiée)

1. Le NIST (National Institute on Standards and Technology) fournit à une entreprise d'informatique A les données suivantes : une courbe elliptique E (donnée par une équation), et des points P et Q sur E, où Q est de la forme aP.
2. Notre ami Bob veut utiliser les services de l'entreprise A, et pour cela il choisit un nombre entier b (par exemple, son mot de passe) que personne (ni l'entreprise A, ni la NSA) ne devrait connaître.

Mais comment fait la NSA ? (version simplifiée)

1. Le NIST (National Institute on Standards and Technology) fournit à une entreprise d'informatique A les données suivantes : une courbe elliptique E (donnée par une équation), et des points P et Q sur E, où Q est de la forme aP.
2. Notre ami Bob veut utiliser les services de l'entreprise A, et pour cela il choisit un nombre entier b (par exemple, son mot de passe) que personne (ni l'entreprise A, ni la NSA) ne devrait connaître. Bob envoie à l'entreprise A le point bP (mais pas l'entier secret b !) pour s'authentifier par exemple.

Mais comment fait la NSA ? (version simplifiée)

1. Le NIST (National Institute on Standards and Technology) fournit à une entreprise d'informatique A les données suivantes : une courbe elliptique E (donnée par une équation), et des points P et Q sur E, où Q est de la forme aP.
2. Notre ami Bob veut utiliser les services de l'entreprise A, et pour cela il choisit un nombre entier b (par exemple, son mot de passe) que personne (ni l'entreprise A, ni la NSA) ne devrait connaître. Bob envoie à l'entreprise A le point bP (mais pas l'entier secret b !) pour s'authentifier par exemple.
3. Comme prévu, A et B connaissent le point abP qui est leur clé secrète pour communiquer sans être espionnés de l'extérieur.

Mais comment fait la NSA ? (version simplifiée)

1. Le NIST (National Institute on Standards and Technology) fournit à une entreprise d'informatique A les données suivantes : une courbe elliptique E (donnée par une équation), et des points P et Q sur E, où Q est de la forme aP.
2. Notre ami Bob veut utiliser les services de l'entreprise A, et pour cela il choisit un nombre entier b (par exemple, son mot de passe) que personne (ni l'entreprise A, ni la NSA) ne devrait connaître. Bob envoie à l'entreprise A le point bP (mais pas l'entier secret b !) pour s'authentifier par exemple.
3. Comme prévu, A et B connaissent le point abP qui est leur clé secrète pour communiquer sans être espionnés de l'extérieur. Pour pouvoir les espionner, il faudrait connaître a ou b...

Mais comment fait la NSA ? (version simplifiée)

1. Le NIST (National Institute on Standards and Technology) fournit à une entreprise d'informatique A les données suivantes : une courbe elliptique E (donnée par une équation), et des points P et Q sur E, où Q est de la forme aP.
2. Notre ami Bob veut utiliser les services de l'entreprise A, et pour cela il choisit un nombre entier b (par exemple, son mot de passe) que personne (ni l'entreprise A, ni la NSA) ne devrait connaître. Bob envoie à l'entreprise A le point bP (mais pas l'entier secret b !) pour s'authentifier par exemple.
3. Comme prévu, A et B connaissent le point abP qui est leur clé secrète pour communiquer sans être espionnés de l'extérieur. Pour pouvoir les espionner, il faudrait connaître a ou b...
4. L'astuce est la suivante : les points P et $Q = aP$ ont été fournis par le NIST à l'entreprise A. Mais évidemment, pour fournir le point Q, le NIST a choisi un entier a et a calculé aP. Donc le NIST connaît l'entier a.

Mais comment fait la NSA ? (version simplifiée)

1. Le NIST (National Institute on Standards and Technology) fournit à une entreprise d'informatique A les données suivantes : une courbe elliptique E (donnée par une équation), et des points P et Q sur E, où Q est de la forme aP.
2. Notre ami Bob veut utiliser les services de l'entreprise A, et pour cela il choisit un nombre entier b (par exemple, son mot de passe) que personne (ni l'entreprise A, ni la NSA) ne devrait connaître. Bob envoie à l'entreprise A le point bP (mais pas l'entier secret b !) pour s'authentifier par exemple.
3. Comme prévu, A et B connaissent le point abP qui est leur clé secrète pour communiquer sans être espionnés de l'extérieur. Pour pouvoir les espionner, il faudrait connaître a ou b...
4. L'astuce est la suivante : les points P et $Q = aP$ ont été fournis par le NIST à l'entreprise A. Mais évidemment, pour fournir le point Q, le NIST a choisi un entier a et a calculé aP. Donc le NIST connaît l'entier a.
5. Problème : le NIST travaille sous le contrôle de la NSA...

Mais comment fait la NSA ? (version simplifiée)

1. Le NIST (National Institute on Standards and Technology) fournit à une entreprise d'informatique A les données suivantes : une courbe elliptique E (donnée par une équation), et des points P et Q sur E, où Q est de la forme aP.
2. Notre ami Bob veut utiliser les services de l'entreprise A, et pour cela il choisit un nombre entier b (par exemple, son mot de passe) que personne (ni l'entreprise A, ni la NSA) ne devrait connaître. Bob envoie à l'entreprise A le point bP (mais pas l'entier secret b !) pour s'authentifier par exemple.
3. Comme prévu, A et B connaissent le point abP qui est leur clé secrète pour communiquer sans être espionnés de l'extérieur. Pour pouvoir les espionner, il faudrait connaître a ou b...
4. L'astuce est la suivante : les points P et $Q = aP$ ont été fournis par le NIST à l'entreprise A. Mais évidemment, pour fournir le point Q, le NIST a choisi un entier a et a calculé aP. Donc le NIST connaît l'entier a.
5. Problème : le NIST travaille sous le contrôle de la NSA...
6. la NSA a donc accès au nombre a : elle peut espionner qui elle veut...

Conclusion

Donc dans cet exemple, le problème n'est pas au niveau des mathématiques, mais au niveau du manque d'indépendance des fournisseurs de certificats de sécurité...

Conclusion

Donc dans cet exemple, le problème n'est pas au niveau des mathématiques, mais au niveau du manque d'indépendance des fournisseurs de certificats de sécurité...

Et on se rend compte sur cet exemple que les mathématiques pures (ou théoriques) sont d'une part assez amusantes et jolies, et d'autres part qu'elles peuvent être très utiles dans la vie quotidienne, pour comprendre certains aspects du monde dans lequel on vit...

Fin

Merci de votre attention !

Fin

Merci de votre attention !

Toutes les questions sont les bienvenues...