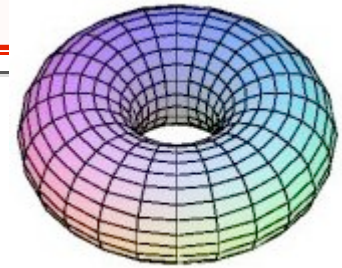


Quand la géométrie vient au secours de l'arithmétique

Le 20 avril 2010, par **Jérôme Gartner**

Allocataire-moniteur de l'université Paris 6 ([page web](#))



La théorie des nombres s'intéresse aux solutions en nombres entiers ou rationnels des équations polynomiales. On sait montrer par exemple que l'on peut écrire 1 comme somme de deux carrés rationnels d'une infinité de façons, que -2 est la différence d'un carré et d'un cube d'une infinité de façons, mais qu'il n'y a qu'un nombre fini de possibilités pour écrire 4 comme différence d'une puissance cinquième et d'un carré. La différence entre ces problèmes est de nature géométrique.

Introduction

« Est-ce que 7 s'écrit comme somme d'un multiple de 2 et d'un multiple de 3 ? » Voici un exemple de question datant de l'antiquité portant sur la théorie des nombres qui est abordé dans l'enseignement secondaire aujourd'hui : ce problème en particulier a une infinité de solutions, et l'on sait toutes les décrire. Ce type de question n'a pas toujours de solution : par exemple, 7 ne peut s'écrire comme somme d'un multiple de 3 et d'un multiple de 6.

D'OÙ vient une telle différence vis à vis du nombre de solutions ? Si on écrit les équations sous-jacentes à ces deux questions, on obtient les énoncés suivants :

Problème 1 Trouver les nombres entiers x et y vérifiant

$$2x + 3y = 7$$

Problème 2 Trouver les nombres entiers x et y vérifiant

$$3x + 6y = 7$$

On peut vérifier que le problème 1 admet pour solution les nombres entiers de la forme $x = 2 - 3k$ et $y = 1 + 2k$ pour tout nombre entier k , et que le problème 2 n'admet pas de solution car s'il en existait, 7 serait divisible par 3.

Solutions rationnelles ou solutions entières ? Une difficulté que présentent les nombres entiers est qu'on ne peut pas en général les diviser. On aimerait pouvoir dire que les solutions de l'équation $2x + 3y = 7$ sont les couples de la forme $(x, \frac{7-2x}{3})$. Reformulons la question originelle de la façon plus générale suivante : trouver les x, y, z entiers tels que

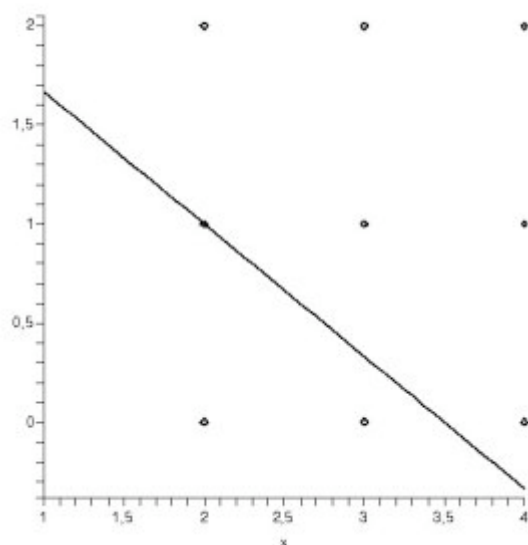
$$2x + 3y = 7z.$$

Les solutions vérifiant $z = 1$ sont exactement les solutions du problème de départ. On remarque que les solutions avec $z \neq 0$ satisfont l'équation plus agréable (car se comportant mieux vis à vis de la division)

$$2\frac{x}{z} + 3\frac{y}{z} = 7$$

On est ainsi ramené à considérer l'équation $2X + 3Y = 7$ dont on cherche les solutions X, Y rationnelles ! Parmi celles-ci, les solutions du problème initial sont celles de dénominateur 1.

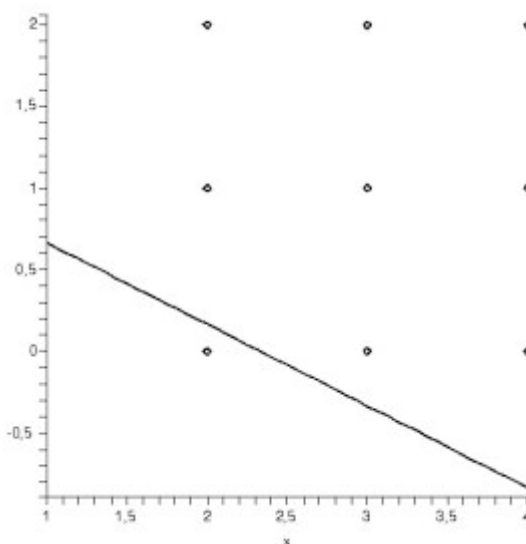
Et la géométrie ?



L'équation du problème 1 a une interprétation connue : les nombres x, y , pris par exemple dans l'ensemble des nombres réels, fournissent les coordonnées des points d'une droite. Traçons les deux droites issues des problèmes 1 et 2 :

La différence entre ces deux droites est que la première passe par des points de coordonnées entières, qui sont de la forme $(2 - 3k, 1 + 2k)$, alors que la deuxième ne passe par aucun point à coordonnée entière. Ceci illustre la géométrie sous-jacente aux problèmes 1 et 2.

Et après ? Dans la suite de cet article, nous allons tenter d'expliquer de quelle manière la géométrie intervient dans la recherche de solutions rationnelles des équations du même type que celle du problème 1 : les équations polynomiales. On va aussi essayer de présenter quelques problèmes qui occupent les chercheurs en théorie des nombres aujourd'hui.



Quelques problèmes polynomiaux

Voici quelques problèmes, rangés suivant leur degré, auxquels on va s'intéresser.

Degré 2

À la question « Comment écrire 1 comme somme de deux carrés rationnels ? », on sait qu'il y a une infinité de possibilités. On sait même plus : on connaît la forme exacte de ces nombres.

Une autre question de ce type est la suivante : « Est-ce que 1 peut s'écrire comme différence d'un carré et du double d'un carré ? ». La réponse est encore oui, et il y a une infinité de solutions. Cette question, reliée à l'équation de Pell-Fermat, admet aussi une réponse précise si on ne considère que les solutions entières. [1]

Degré 3

Il est possible de montrer que -2 est différence d'un carré et d'un cube rationnels d'une infinité de manière. Mais contrairement aux cas précédents, ce n'est pas seulement la valeur du degré qui dicte le comportement des solutions. Par exemple, l'équation $y^2 = x^3 + x$ a exactement 3 solutions rationnelles. Ici, suivant les cas, on aura donc un nombre fini ou une infinité de solutions, toutes exprimables à partir de quelques solutions fondamentales. [2]

Degré 5

Il n'existe qu'un nombre fini de manières d'écrire 4 comme différence d'un carré par une puissance cinquième. Aucune équation de ce type n'admet une infinité de solutions rationnelles... Pourquoi ?

Mise en équation

Les exemples cités ci-dessus ont ceci en commun : on cherche les solutions, d'une équation de type *polynomial*. Dire que -2 est différence d'un carré et d'un cube, c'est démontrer qu'il existe deux nombres rationnels x et y tels que

$$y^2 - x^3 = -2$$

Les exemples du paragraphe précédent correspondent aux équations :

$$x^2 + y^2 - 1 = 0 \quad (1)$$

$$x^2 - 2y^2 - 1 = 0 \quad (2)$$

$$y^2 - x^3 + 2 = 0 \quad (3)$$

$$y^2 - x^3 - x = 0 \quad (4)$$

$$y^2 - x^5 - 4 = 0 \quad (5)$$

Les solutions de l'équation (1) sont les couples $\left(\frac{2nm}{n^2+m^2}, \frac{n^2-m^2}{n^2+m^2}\right)$ et $\left(\frac{n^2-m^2}{n^2+m^2}, \frac{2nm}{n^2+m^2}\right)$, où n et m sont deux nombres entiers.

Les solutions entières de l'équation (2) sont les couples (x_n, y_n) pour n entier strictement

positif, où (x_1, y_1) est la solution évidente $(3, 2)$ et (x_n, y_n) est tel que $x_n + y_n\sqrt{2} = (3 + 2\sqrt{2})^n$.

Les solutions de l'équation (3) sont obtenues à partir de la solution fondamentale $(3, 5)$, en itérant une formule un peu compliquée.

Les solutions rationnelles de l'équation (4) sont exactement $(0, 0)$, $(0, 1)$, $(0, -1)$. Montrer que ces trois couples sont solution est simple, mais il est en revanche difficile de montrer que ce sont les seules !

Le couple $(6, 2)$ est solution de l'équation (5), et on sait qu'il n'y a qu'un nombre fini de solutions rationnelles. Mais combien ? Comment être sûr qu'on les a toutes trouvées ?

L'arbre des possibles

Étant donnée une équation polynomiale du type

$$y^2 = f(x) := a_0 + a_1x + \dots + a_nx^n,$$

le théoricien des nombres va chercher à déterminer dans quelle situation se place le problème.

- L'équation admet un nombre fini de solutions.
 - Que l'on sait compter et/ou déterminer.
 - Dont on ne sait rien.
- L'équation admet une infinité de solutions.
 - Que l'on sait déterminer simplement (i.e. à partir d'opérations élémentaires et d'un nombre fini de solutions « de base »).
 - Dont on ne sait rien.

On cherche donc dans un premier temps à savoir s'il y a une infinité ou non de solutions, puis, s'il est possible de les décrire (de les dénombrer s'il y en a un nombre fini, de savoir comment les engendrer s'il y en a une infinité). Comme l'aura laissé penser la liste des exemples ci-dessus, le comportement des solutions d'une équation polynomiale dépend en partie du degré de l'équation.

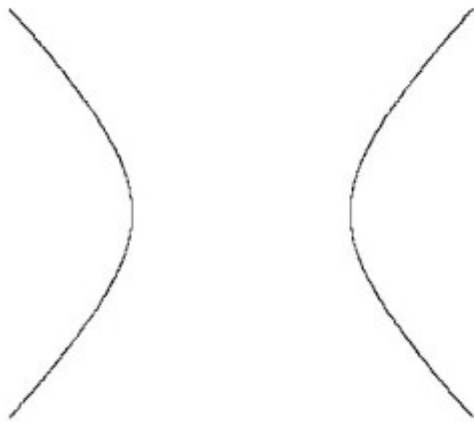
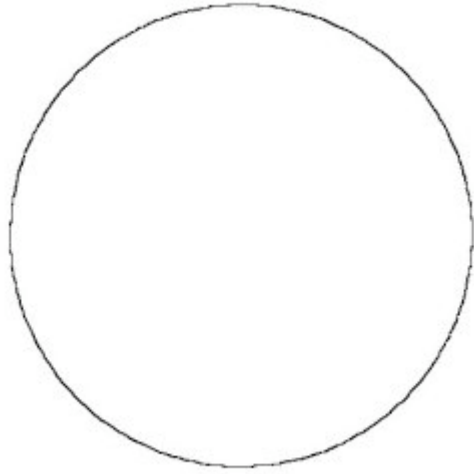
Une fausse bonne idée

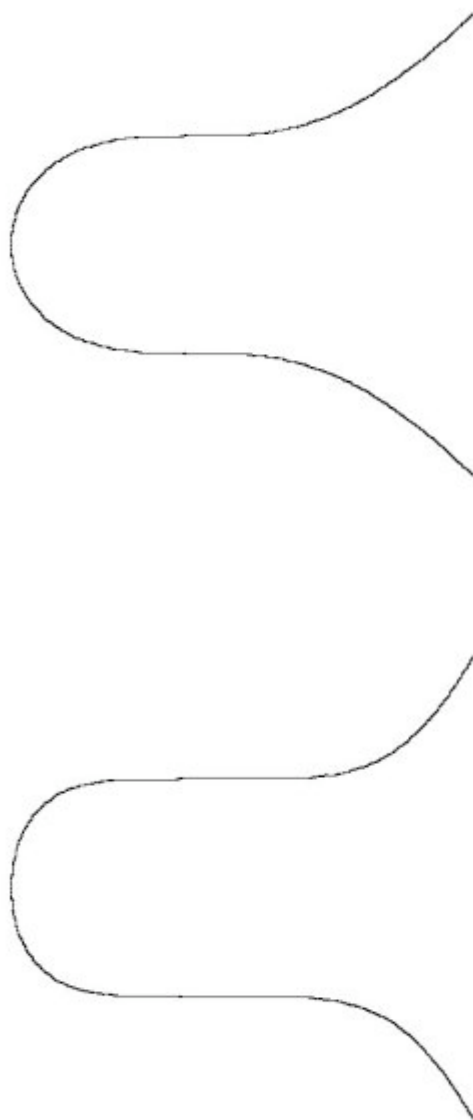
Il serait tentant d'annoncer que le nombre de solutions rationnelles d'une équation polynomiale est dictée par son degré. En particulier, à la vue des quelques exemples exposés, on a envi de dire que si le degré de l'équation est grand, celle-ci n'admet qu'un nombre fini de solutions rationnelles. Ceci est *faux* ! L'équation $y^2 = x^{57} - x^{56}$, de degré 57, a une infinité de solutions rationnelles. [3]

C'est en fait une propriété des équations polynomiales plus géométrique, *son genre* qui détermine la quantité de solutions rationnelles.

Traçons les solutions réelles de ces équations, c'est-à-dire repérons dans le plan muni de coordonnées les points dont les coordonnées (x, y) satisfont les équations ci-dessus.

On obtient les courbes suivantes :





Le genre d'une courbe

Supposons maintenant que les variables x, y des équations que l'on considère sont les plus générales possibles : des nombres complexes. On écrit sous forme inconnue $x = a + ib$, $y = c + id$, ce qui donne après simplification les systèmes d'équations suivants, correspondants respectivement aux équations (1), (3) et (5) :

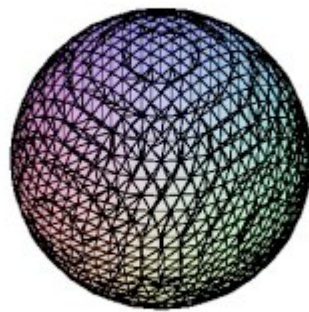
$$\begin{cases} a^2 - b^2 + c^2 - d^2 & = & 1 \\ ab + cd & = & 0 \end{cases} \quad (6)$$

$$\begin{cases} -a^3 + 3ab^2 + c^2 - d^2 & = & -2 \\ -3a^2b + b^3 + 2cd & = & 0 \end{cases} \quad (7)$$

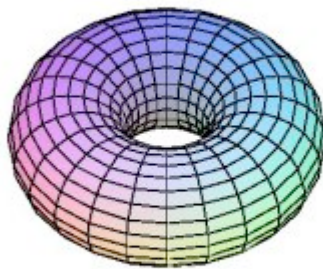
$$\begin{cases} -a^5 + 10a^3b^2 - 5ab^4 + c^2 - d^2 & = 4 \\ -5a^4b + 10a^2b^3 - b^5 + 2cd & = 0 \end{cases} \quad (8)$$

Ce sont des systèmes de deux équations à 4 inconnues : ces systèmes représentent des surfaces dans un espace de grande dimension, ici 4. [4]

Un aspect du métier de mathématicien est de *classifier* les objets suivant divers propriétés. Supposons par exemple que l'on s'autorise à déformer les surfaces *sans les déchirer*. Les surfaces les plus simples obtenues par déformations à partir des surfaces (6), (7) et (8) ci-dessus [5] auront alors les apparences suivantes :



Surface (6)



Surface (7)



Surface (8)

Que remarque-t-on ? Suivant les cas, on obtient des surfaces à 0, 1 ou 2 trous. Ce nombre de trous est un invariant mathématique, appelé le *genre* d'une surface. Il se trouve que cet invariant géométrique a un lien profond avec le nombre de solutions rationnelles des équations d'origine : ce lien a été conjecturé par Mordell dans les années 1920 et démontré par Faltings en 1983.

Lien avec le degré Dans le cas des équations du type $y^2 = a_0 + a_1x + \dots + a_nx^n$, il existe un lien entre le genre g de la surface associée et son degré n si l'équation $a_0 + a_1x + \dots + a_nx^n = 0$ a exactement n solutions distinctes. On a dans ce cas $n = 2g + 1$ ou $n = 2g + 2$. Mais attention, ce lien n'existe pas en général : l'équation $y^2 = x^n - x^{n-1}$ est de degré n mais son genre g est nul !

La conjecture de Mordell

Considérons une équation polynomiale à coefficients rationnels, dont on cherche les solutions rationnelles. On peut lui associer comme ci-dessus un genre, qui correspond au nombre de trous apparaissant sur la surface définie par l'équation dans un espace de dimension 4. Le théorème de Faltings s'énonce alors ainsi : « Si le genre est supérieur ou égal à 2, l'équation n'admet qu'un nombre fini de solutions rationnelles ». [6]

Ce théorème a une application bien connue des théoriciens des nombres au problème de Fermat : il a permis (avant les travaux de Wiles de 1995) de savoir que l'équation de Fermat $x^n + y^n = 1$ n'avait qu'un nombre fini de solutions rationnelles si $n \geq 4$.

Une question ouverte

Le théorème de Faltings implique qu'il n'y a qu'un nombre fini de solutions rationnelles à une équation du type Fermat. Une méthode simple pour les trouver serait d'essayer tous les nombres rationnels un à un et de voir lesquels sont solutions. Une telle méthode n'a de chance d'aboutir

que si l'on sait jusqu'où aller. Par exemple, si on sait que les solutions de l'équation $x^5 + y^5 = 1$ ont toutes un numérateur et un dénominateur plus petit que 5000000, un ordinateur testera rapidement toutes les possibilités pour montrer que les seules solutions sont $(1, 0)$ et $(0, 1)$. [7]

La question de trouver une borne sur le numérateur et le dénominateur des solutions d'une équation correspond à un problème d'effectivité, c'est-à-dire de « faisabilité ». C'est un problème difficile : il n'a pas de solution satisfaisante à ce jour. La solution à cette question ouvrirait des perspectives plus larges : par exemple, si ce problème est résolu, alors la célèbre conjecture *abc* est prouvée ! [8]

Le cas particulier des courbes elliptiques

Les chercheurs n'ont pas seulement des problèmes avec les « équations de genre supérieur à 2 », mais aussi avec celles de genre 1. Ces équations, qui correspondent à ce qu'on appelle des *courbes elliptiques* se mettent sous la forme $y^2 = x^3 + bx + c$. On sait alors qu'il y a une alternative : soit le nombre de solutions est fini, et dans ce cas on peut parfois connaître leur nombre, soit il y a une infinité de solutions, qui s'obtiennent à partir d'un nombre fini de solutions « fondamentales » à l'aide d'opérations explicites.

A l'heure actuelle on ne sait pas grand chose des solutions fondamentales. Pour une équation donnée, on ne sait facilement déterminer ni le nombre de solutions fondamentales, ni leurs expressions. Dans le cas où on sait qu'il n'y a qu'une solution fondamentale, une méthode dite *des points de Heegner* permet éventuellement d'explicitier cette solution particulière. Une branche active de la recherche actuelle se penche sur ces problèmes particuliers. [9]

[D] **H. Darmon**, *Rational points on modular elliptic curves*, 2001.

[H] **M. Hindry**, *Arithmétique*, Calvage et Mounet, 2009.

[ST] **J. Silverman, J. Tate**, *Rational points on elliptic curves*, Springer 1992.

[HS] **M. Hindry, J. Silverman**, *Diophantine geometry : an introduction*, Springer 2000.

[Z] **Don Zagier**, *Modular points, modular curves, modular surfaces and modular forms*, Springer LNM 1111.

Notes

[▲1] Le lecteur intéressé trouvera une étude poussée des équations de Pell-Fermat dans le livre de Marc Hindry [H].

[▲2] Le livre de Marc Hindry [H] cité ci-dessus fournit une introduction aux courbes elliptiques. On peut aussi consulter le livre de J. Silverman et J. Tate [ST].

[▲3] Les solutions de cette équation sont exactement les couples $(1 + t^2, (1 + t^2)^{28}t)$ où t est un nombre rationnel.

[▲4] On pourra se référer par exemple à l'article **Le h -principe de Misha Gromov** de **Michèle Audin** et **Pierre Pansu** sur le site pour comprendre ce qu'est une immersion.

[▲5] modulo quelques points à l'infini

[▲6] Une preuve de ce théorème se trouve dans le livre de M. Hindry et J. Silverman [HS]. On peut aussi télécharger une vidéo de H. Darmon sur le **site**

[▲7] Quelques problèmes ouverts de géométrie diophantienne sont exposés dans le livre de M. Hindry et J. Silverman [HS].

[▲8] Concernant la conjecture abc , le livre de M. Hindry [H] en donne aperçu.

[▲9] Le livre de H. Darmon [D] disponible **ici** explique ce que sont les points de Heegner et donne des conjectures pour généraliser leur construction. Pour des exemples, on peut conseiller de ce reporter à l'article de Don Zagier [Z].

► **Crédits images**

Pour citer cet article : **Jérôme Gartner**, **Quand la géométrie vient au secours de l'arithmétique**. *Images des Mathématiques*, CNRS, 2010. En ligne, URL : <http://images.math.cnrs.fr/Quand-la-geometrie-vient-au.html>