Équations diophantiennes et courbes elliptiques

Nicolas Billerey, Marusia Rebolledo

L'étude des équations diophantiennes remonte à l'antiquité grecque. Elles doivent leur nom au mathématicien Diophante d'Alexandrie, qui vivait au 3e siècle, pour son traité d'Arithmétique concernant ces questions. Une *équation diophantienne* est une équation polynomiale à coefficients entiers dont on cherche les solutions en nombres entiers (positifs ou négatifs) ou en nombres rationnels (c'est-à-dire des fractions p/q où p, q sont des entiers). Par exemple, une équation diophantienne linéaire (c'est-à-dire de degré 1) en deux variables x et y est une équation de la forme

$$ax + by = c$$

avec a, b, c entiers. C'est l'équation d'une droite du plan. Chercher les solutions (x, y) entières c'est donc chercher les points à coordonnées entières de cette droite ; autrement dit, dans un repère orthonormé, c'est chercher quand cette droite coupe les noeuds d'un quadrillage formé de carreaux de côtés de longueur 1.

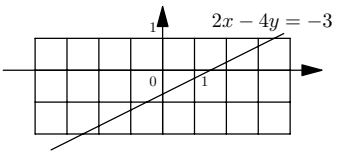

FIGURE 1 – Equation diophantienne linéaire $ax + by = c$.

On peut également considérer des équations de *degré* plus grand ou ayant un plus grand nombre de variables. Par exemple, l'équation suivante a deux inconnues et est de degré 2 :

$$x^2 + y^2 = 1. \tag{1}$$

C'est l'équation du cercle de centre O et de rayon 1 dans un repère orthonormé d'origine O. Déterminer les solutions entières (x, y) de (1) c'est déterminer l'ensemble des points de ce cercle qui sont aux noeuds du réseau.

En ajoutant une variable, on peut considérer l'équation

$$x^2 + y^2 = z^2 \tag{2}$$

qui est intimement liée à la précédente. En effet si (x, y, z) est une solution de (2) avec $z \neq 0$ alors $(x/z, y/z)$ est une solution rationnelle de (1). Inversement toute solution rationnelle de (1) donne lieu à une solution entière de (2). Les triplets d'entiers (x, y, z) solutions de (2) sont appelés *triplets pythagoriciens* en référence à Pythagore : x, y, z sont alors en effet les côtés entiers d'un triangle rectangle. Par exemple, $(3, 4, 5)$ est un triplet Pythagoricien.

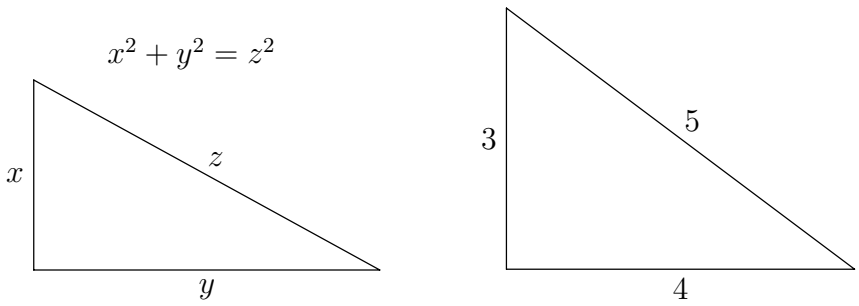

FIGURE 2 – Triplets pythagoriciens.

Lorsqu'on augmente la puissance des inconnues dans l'équation précédente, on obtient la maintenant célèbre *équation de Fermat*

$$x^n + y^n = z^n \tag{3}$$

où n est un entier fixé plus grand que 2. Cette équation est un bon exemple de la difficulté de résolution de certaines équations diophantiennes. Au dix-septième siècle, Fermat a conjecturé que lorsque $n \geq 3$, l'équation (3) n'admettait pas de solution entière *non triviale* c'est-à-dire autre que celles pour lesquelles l'un des entiers x, y, z est nul. Il fallut les travaux de nombreux mathématiciens, l'introduction et le développement de techniques sophistiquées à la croisée de plusieurs domaines des mathématiques (algèbre, géométrie arithmétique, analyse) avant de pouvoir démontrer cette conjecture. La preuve de Wiles (1995), complétée par les travaux de Breuil, Conrad, Diamond, Taylor a été également fertile pour la résolution d'autres équations diophantiennes de la même famille. Les *courbes elliptiques* dont nous parlerons plus loin tiennent un rôle essentiel dans la preuve du théorème de Fermat.

Revenons à l'écriture générale d'une équation diophantienne :

$$f(x_1, \ldots, x_m) = 0 \tag{4}$$

où f est un *polynôme* en m indéterminées à coefficients entiers. On cherche les solutions $(x_1, \ldots, x_m)$ où les x_i sont soit des entiers, soit des rationnels.

Etant donné une équation du type (4), on peut se poser les questions suivantes :

Q1. L'équation (4) admet-elle des solutions entières (ou rationnelles) ?

Q2. Peut-on déterminer s'il y a un nombre fini ou infini de solutions ? Si ce nombre est fini, peut-on en donner une borne ?

Q3. Peut-on toutes les déterminer, c'est-à-dire en faire la liste si elles sont en nombre fini ou bien en donner une *paramétrisation* si elles sont en nombre infini ? Peut-on à partir d'une ou plusieurs solutions données, déterminer toutes les autres ?

Malheureusement, il est impossible de répondre ne serait-ce qu'à la question Q1 en toute généralité. En effet, dans la lignée des travaux antérieurs de Davis, Putnam et Robinson, Matiyasevich donne en 1970 une réponse définitive au dixième des célèbres vingt-trois problèmes de Hilbert énoncés au Second Congrès International de Mathématiques de 1900 [Hil00, GG00] :

Théorème 1 (Matiyasevich)**.** *Il n'existe pas d'algorithme général prédisant si une équation diophantienne donnée admet des solutions (entières).*

Cependant, s'il n'existe pas d'algorithme valable pour une équation générale, demeure l'espoir d'élaborer des méthodes pour certaines classes d'équations particulières. Voir [DMR76, Mat99]. Dans la suite de cet article, nous allons donner un aperçu des cas pour lesquels on dispose de méthodes maintenant classiques de résolution. Nous allons également donner une idée des raisons pour lesquelles ces méthodes, élaborées au cas par cas pour des classes particulières d'équations, ne fonctionnent pas pour d'autres et comment, dès le degré 3 pour deux variables (c'est le cas des courbes elliptiques), de réelles difficultés apparaissent.

On peut imaginer que la difficulté de résolution augmente avec le nombre de variables et le degré de l'équation. Commençons par considérer une équation diophantienne en une variable

$$a_0 + a_1 x + \cdots + a_n x^n = 0 \tag{5}$$

avec $a_0, \ldots, a_n$ des entiers. Supposons qu'un rationnel x soit une solution de (5). Ecrivons $x = p/q$ avec p, q deux entiers premiers entre eux (c'est-à-dire n'admettant d'autre diviseur commun (positif) que 1). Alors en multipliant (5) par q^n on obtient l'égalité

$$a_0 q^n + a_1 p q^{n-1} + \cdots + a_n p^n = 0$$

ce qui montre que $a_0 q^n$ est multiple de p. Le *lemme de Gauss* certifie alors que p divise l'entier a_0 puisque p et q sont premiers entre eux. L'entier p ne peut alors prendre qu'un nombre fini de valeurs (les diviseurs de a_0). De la même façon, on peut montrer que q divise l'entier a_n et q prend alors un nombre fini de valeurs possibles. On peut ainsi faire une liste finie des valeurs possibles pour les solutions rationnelles de (5) (et donc des solutions entières) et il suffit ensuite de tester chacune de ces valeurs pour voir si elle est ou non réellement solution de (5). On obtient donc un algorithme très simple pour résoudre les équations diophantiennes en une variable, quel que soit leur degré.

Augmentons le nombre de variables mais restons en degré 1 en revenant à notre tout premier exemple d'équation diophantienne

$$ax + by = c \tag{6}$$

avec a, b, c entiers. Là encore, des résultats d'arithmétique élémentaire nous permettent de conclure. En effet, si (x, y) est un couple d'entiers vérifiant (6), alors tout diviseur commun de a et b divise également c et par conséquent le plus grand diviseur commun d de a et b (le *pgcd*) divise c. Inversement supposons que d divise c, alors on peut écrire une nouvelle égalité

$$a'x + b'y = c' \quad \text{où} \quad a' = \frac{a}{d},\ b' = \frac{b}{d},\ c' = \frac{c}{d},$$

mais à présent les entiers a' et b' sont premiers entre eux. Le théorème de Bézout affirme alors qu'il existe deux entiers u, v tels que $a'u + b'v = 1$. Ces entiers u, v ainsi que le pgcd d de a et b peuvent être déterminés par un algorithme classique et peu coûteux appelé *algorithme d'Euclide*. En multipliant cette identité de Bézout par $c' = \frac{c}{d}$, nous disposons alors d'une solution particulière de (6) : $(x_0, y_0) = (u\frac{c}{d}, v\frac{c}{d})$. Nous avons ainsi répondu à la question Q1 : l'équation (6) admet une solution entière si et seulement si le pgcd de a et b divise c. De plus si c'est le cas, toute autre solution (x, y) vérifie $a'(x-x_0)+b'(y-y_0) = 0$. Le lemme de Gauss invoqué plus haut montre alors que b' divise $x - x_0$ donc x, y s'écrivent sous la forme $x = x_0 + kb', y = y_0 - ka'$ pour k entier. On vérifie inversement que des entiers de cette forme sont solutions de (6). On a ainsi répondu aux questions Q1, Q2, Q3 dans leur totalité en déterminant explicitement l'ensemble (infini) des solutions quand elles existent.

Les équations diophantiennes de degré 1 avec plus de deux inconnues entières peuvent être résolues par des méthodes analogues.

Le cas du degré 2 devient plus difficile. Limitons-nous au cas de deux inconnues x, y et considérons pour commencer l'exemple du cercle d'équation

$$x^2 + y^2 = 1. \tag{7}$$

Cette équation admet des solutions rationnelles, par exemple $(1,0), (0,1), (0,-1), (-1,0)$, ce qui répond à la question Q1 (ce sont en fait les seules solutions entières). Choisissons une solution particulière, par exemple $(-1,0)$ et traçons une droite passant par le point P ayant cette solution comme coordonnées. Cette droite, si elle n'est pas tangente au cercle c'est-à-dire ici si elle n'est pas verticale, recoupera le cercle en un seul autre point que nous noterons Q_t. Inversement par P et tout point du cercle distinct de P, il passe une seule droite et celle-ci n'est pas tangente au cercle.

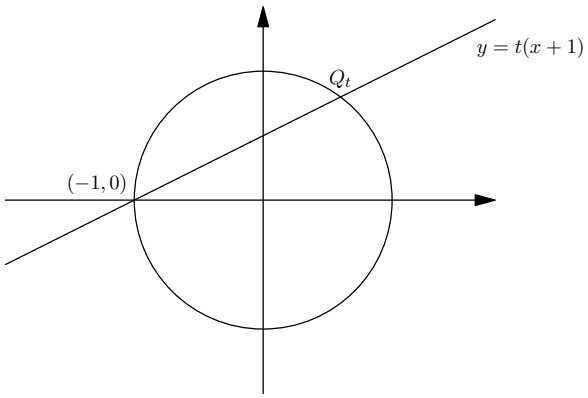

FIGURE 3 – Equation $x^2 + y^2 = 1$. Méthode des cordes.

Il reste donc à déterminer quelles sont les droites issues de P qui intersectent le cercle en des points à coordonnées rationnelles. Une droite non tangente au cercle passant par P a une équation de la forme $D_t : y = t(1+x)$ où t est un nombre réel (c'est la pente de la droite). Le nombre réel t est un *paramètre* : en faisant varier t, on obtient toutes les droites possibles (non tangentes au cercle et passant par le point P de coordonnées $(-1,0)$). En reportant la relation donnée par D_t dans (7), on montre que la droite D_t recoupe le cercle au point Q_t de coordonnées

$$\left(\frac{1-t^2}{1+t^2}, \frac{2t}{t^2+1}\right). \tag{8}$$

Lorsque D_t a une équation rationnelle, c'est-à-dire lorsque t est rationnel, le point ci-dessus est à coordonnées rationnelles. Il est aisé de voir qu'inversement si Q_t est un point rationnel alors la droite (Q_tP) a une équation rationnelle. On obtient ainsi une *paramétrisation* de l'ensemble (infini) des solutions de (7) à partir d'une solution triviale de départ, ce qui répond aux questions Q2 et Q3. (Le point $(-1,0)$ étant obtenu en faisant tendre t vers l'infini).

La méthode décrite ci-dessus, appelée aujourd'hui *méthode des cordes*, a été introduite par Diophante pour paramétrer les triplets pythagoriciens, même s'il faut attendre Descartes et Pascal et l'introduction des coordonnées cartésiennes pour avoir une telle interprétation géométrique. Le lecteur pourra se référer à [ST92] ou [Kna92] pour la paramétrisation exacte des triplets pythagoriciens et pour un exposé plus détaillé de la méthode des cordes.

Cette méthode se généralise à certaines équations diophantiennes de degré 2 quelconques (en deux variables)

$$ax^2 + bxy + cy^2 + dx + ey + f = 0.$$

Une équation de cette forme est l'équation d'une *conique* $\mathcal{C}$ du plan. Supposons que $\mathcal{C}$ admette un point rationnel $P = (x_0, y_0)$. Si $\mathcal{C}$ est *non degenerée*, toute droite rationnelle passant par P et non tangente à la courbe recoupera la conique en un point rationnel. Cela permet de nouveau de paramétrer l'ensemble des solutions rationnelles de l'équation diophantienne à partir d'une solution particulière P et donc de répondre aux questions Q2 et Q3.

Cependant, qu'en est-il de la question Q1 ? Existe-t-il toujours des solutions aux équations diophantiennes quadratiques et si oui, comment en déterminer une ? Malheureusement, certaines coniques n'ont pas de point rationnel. C'est le cas, par exemple, du cercle d'équation

$$x^2 + y^2 = 3.$$

Montrons-le par un raisonnement par l'absurde. Supposons qu'il y en ait un : nous pouvons l'écrire $(x = X/Z, y = Y/Z)$ où X, Y, Z sont des entiers qui vérifient alors

$$X^2 + Y^2 = 3Z^2. \tag{9}$$

Quitte à diviser par les facteurs communs, nous pouvons supposer que X, Y, Z sont premiers entre eux dans leur ensemble (c'est-à-dire n'ont pas de diviseur commun autre que 1). D'après (9), 3 divise $X^2 + Y^2$. Il s'ensuit que si 3 divisait X alors 3 diviserait également $Y^2 = (X^2 + Y^2) - X^2$ donc par le lemme d'Euclide, 3 diviserait Y (puisque 3 est un nombre premier). Mais dans ce cas, 3^2 diviserait $3Z^2$ et donc 3 diviserait Z. Ainsi si 3 divise X alors 3 divise aussi Y et Z ce qui est impossible puisque X, Y, Z ont été supposés premiers entre eux. Donc 3 ne divise pas X. Pour les mêmes raisons, 3 ne divise pas Y. Mais alors regardons ce qui se passe *modulo* 3 : les valeurs possibles de X et Y modulo 3 sont 1 et -1 donc $X^2 + Y^2 \equiv 2 \pmod 3$. D'un autre côté $3Z^2 \equiv 0 \pmod 3$. Comme $0 \not\equiv 2 \pmod 3$, cela aboutit à une contradiction prouvant ainsi que (9) n'a pas de solution rationnelle, comme annoncé.

L'argument ci-dessus revient à dire que si l'équation (9) a une solution entière alors elle admet une solution modulo 3. Comme ce n'est pas le cas, (9) n'a pas de solution entière.

Ce principe est vrai en plus grande généralité. Legendre (1752-1833) a en effet montré que l'équation

$$aX^2 + bY^2 = cZ^2$$

a une solution entière non nulle si et seulement si la congruence

$$aX^2 + bY^2 \equiv cZ^2 \mod m$$

a une solution en entiers premiers à m où m est un certain entier lié à a et b (pour plus de details voir par exemple [ST92]). Hasse a étendu cette méthode pour le cas de $n \geq 3$ variables. C'est le *principe de Hasse* : une équation diophantienne *homogène*[1] de degré 2 en n variables a une solution entière non nulle si et seulement si elle admet une solution réelle et une solution en *entiers $p-$adiques*[2] pour tout nombre premier p.

Cela donne un algorithme pour tester si une conique admet ou non des points rationnels, répondant ainsi (en un temps fini) à la question Q1.

Nous avons vu que nous disposons de méthodes pour étudier les équations diophantiennes de degré 1 et 2. Il est naturel de voir si celles-ci s'appliquent à l'étude des équations diophantiennes de degré 3 en deux variables, c'est-à-dire des équations de la forme

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0,$$

1. Un polynôme f en n variables est *homogène de degré k* s'il vérifie $f(\lambda x_1, \ldots, \lambda x_n) = \lambda^k f(x_1, \ldots, x_n)$.
2. On ne définira pas ici ce qu'est un entier $p-$adique.

où $a, b, c, d, e, f, g, h, i, j$ sont des nombres entiers fixés. Une équation de cette forme est l'équation d'une *cubique*Â du plan. Par exemple, l'équation diophantienne $x^3 + y^3 = 1$ qui est le premier cas de l'équation de Fermat (3), résolue par Fermat lui-même, est l'équation d'une cubique.

Sur les figures 4 et 5, on a représenté dans le plan l'ensemble des couples (x, y) de nombres réels solutions de deux équations cubiques particulières.

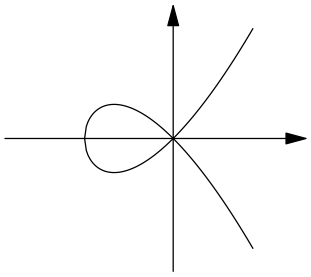

FIGURE 4 – $y^2 = x^3 + x^2$.

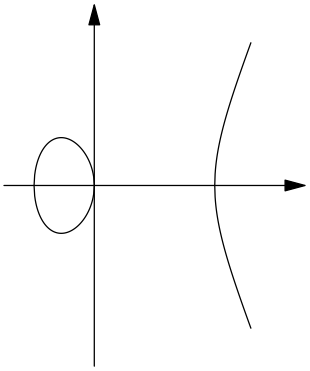

FIGURE 5 – $y^2 = x^3 - x^2 - 2x$.

Nous allons voir que de telles équations diophantiennes ne se laissent pas appréhender aussi facilement que l'étude des équations de degré 1 ou 2 (en deux variables) pourrait le laisser penser. Les cubiques, et plus particulièrement celles d'entre elles que l'on appelle courbes elliptiques [3], constituent un bon exemple d'objet mathématique simple dont l'étude nécessite de faire appel à des outils issus de branches des mathématiques aussi variées que la géométrie, l'arithmétique ou l'algèbre. Si l'apport de la géométrie ou de l'arithmétique ne devrait pas surprendre le lecteur [4], celui de l'algèbre est plus déroutant. Nous allons en donner un aperçu.

On a vu plus haut l'élégante réponse que le principe de Hasse apporte à la question Q1 dans le cas des coniques. Malheureusement celui-ci ne fonctionne plus pour les cubiques. Selmer a en effet donné en 1951 un contre-exemple à ce principe : la cubique d'équation $3X^3+4Y^3+5Z^3 = 0$ n'admet d'autre solution entière que $(0, 0, 0)$ et pourtant l'équation de congruence $3X^3 + 4Y^3 + 5Z^3 \equiv 0 \pmod{m}$ admet des solutions en nombres entiers premiers entre eux quel que soit m.

D'autre part, même lorsqu'on considère une cubique ayant un point rationnel et qu'on essaie de lui appliquer la méthode des cordes qui s'est avérée si fructueuse pour répondre aux questions Q2 et Q3 dans le cas des coniques, on se heurte de nouveau à une difficulté. En effet, une droite issue d'un point d'une cubique la recoupe généralement en non pas un mais deux autres points. C'est ici que l'algèbre intervient. Supposons que l'on dispose de deux points P et Q à coordonnées rationnelles sur une cubique $\mathcal{C}$ donnée. Alors, la droite joignant P à Q coupe $\mathcal{C}$ en un troisième point, noté $P \star Q$, dont les coordonnées sont elle-mêmes rationnelles [5]. Grâce à cette observation, il est possible de munir l'ensemble $\mathcal{C}(\mathbf{Q})$ des points de $\mathcal{C}$ à coordonnées rationnelles d'une « loi », appelée loi de composition interne et notée $\oplus$, dont les propriétés sont tout à fait

3. Il s'agit de cette classe particulière de cubiques qui sont « lisses » (de façon imagée, cela signifie que leur graphe ne fait pas apparaître de point de rebroussement ou de croisement) et qui possèdent au moins une solution rationnelle. La cubique de la figure 4 n'est pas une courbe elliptique, contrairement à celle de la figure 5.

4. Après tout ce sont bien des courbes planes données par des équations polynomiales.

5. Lorsque les points P et Q sont confondus, on prendra la tangente. Pour que ce procédé s'applique, il est nécessaire de travailler avec une cubique « projective ». Sur la courbe elliptique de la figure **??** par exemple, cela revient à rajouter un point situé à l'infini dans la direction verticale et dont on décrète qu'il est le troisième point d'intersection de la cubique avec la droite passant par deux points de même abscisse.

analogues à celles de l'addition dans l'ensemble des entiers relatifs. Cette structure algébrique, connue sous le nom de *groupe commutatif* et dont la formulation remonte à Galois, confère aux courbes elliptiques une extraordinaire richesse dont on peut tirer profit pour l'étude de leurs points rationnels.

La figure 6 illustre le fonctionnement de cette « addition » d'un type particulier. On commence pas isoler un point rationnel $\mathcal{O}$ de $\mathcal{C}$ appelé origine (et dont le rôle est l'analogue du zéro dans les entiers). L'addition $P \oplus Q$ de deux points P et Q n'est alors rien d'autre que le troisième point d'intersection de $\mathcal{C}$ avec la droite passant par $\mathcal{O}$ et $P \star Q$ [6].

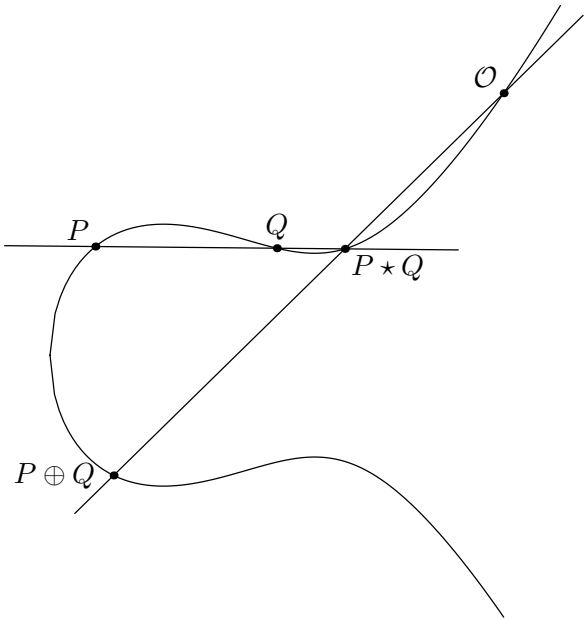

FIGURE 6 – L'addition sur les courbes elliptiques.

Le lecteur curieux pourra s'amuser à vérifier sur la figure proposée les propriétés suivantes de la loi $\oplus$: pour tous points P, Q, R de $\mathcal{C}$,

1. on a $P \oplus \mathcal{O} = \mathcal{O} \oplus P = P$;
2. il existe P' tel que $P \oplus P' = P' \oplus P = \mathcal{O}$;
3. on a $P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$;
4. on a $P \oplus Q = Q \oplus P$.

Partant d'un point P de $\mathcal{C}(\mathbf{Q})$, on peut alors considérer tous ses « multiples » pour la loi $\oplus$: P, $P \oplus P$, $P \oplus P \oplus P$,... que l'on note P, $2P$, $3P$, etc. On a deux cas de figure : soit on retombe sur le point P dont on est parti et le cycle reprend, soit, au contraire, on ne revient jamais au point de départ et on engendre alors une infinité de points distincts. Dans le premier cas, on parle de point d'ordre fini et dans le second d'ordre infini. En 1922, Louis Mordell [7] (voir [Mor22]), a démontré le résultat suivant : il existe un ensemble fini de points $P_1, \ldots, P_m$ de $\mathcal{C}(\mathbf{Q})$ ayant la propriété que tout point de $\mathcal{C}(\mathbf{Q})$ s'écrit comme somme finie, pour la loi $\oplus$, de multiples de $P_1, \ldots, P_m$. On dit que le *groupe* $\mathcal{C}(\mathbf{Q})$ est *engendré* par les points $P_1, \ldots P_m$ de $\mathcal{C}(\mathbf{Q})$. L'ensemble $\mathcal{C}(\mathbf{Q})$ est

6. En particulier, lorsque P, Q et $\mathcal{O}$ sont alignés, on a $P \oplus Q = \mathcal{O}$ ou encore, $P = -Q$.
7. Ce résultat fut plus tard repris et généralisé par André Weil en 1930.

fini si tous les points $P_1, \ldots, P_m$ sont d'ordre fini et il est infini sinon. Ce résultat, qui fournit en théorie une réponse aux questions Q2 et Q3 pour les courbes elliptiques, est malheureusement non effectif : il n'y a actuellement pas d'algorithme ou de théorie permettant de calculer un entier minimal r et de produire un ensemble de points $P_1, \ldots, P_r$ engendrant tous les points d'ordre infini de $\mathcal{C}(\mathbf{Q})$. Ce problème fait l'objet d'une conjecture très importante énoncée par deux mathématiciens britanniques Bryan Birch et Peter Swinnerton-Dyer et pour laquelle le Clay Mathematics Institute a proposé en l'an 2000 un prix d'un montant d'un million de dollars. On pourra lire à ce sujet l'exposé introductif d'Andrew Wiles lors de la présentation des *Millenium Problems* [Wil06].

Ce qui précède donne un aperçu de la richesse de la théorie des équations diophantiennes et plus particulièrement des courbes elliptiques, ainsi que de l'étendue des questions qui demeurent ouvertes et font l'objet des recherches actuelles. Le lecteur désireux d'aller plus loin pourra par exemple consulter [ST92] dont nous nous sommes largement inspirés pour cet article.

Si elle fait indéniablement partie des mathématiques fondamentales, la théorie des courbes elliptiques a des applications aussi bien théoriques que très concrètes. Mentionnons pour finir deux exemples illustrant ceci. Pour plus de détails, on pourra par exemple se référer à l'article de Guy Henniart [Hen09] sur les nombres congruents ou le livre de William Stein [Ste09] [8] pour les deux exemples évoqués.

Le problème des nombres congruents. On dit qu'un nombre entier n est congruent s'il est l'aire d'un triangle rectangle de côtés de longueur rationnelle. De façon équivalente, cela revient à dire que le système d'équations

$$\begin{cases} a^2 + b^2 &= c^2 \\ \frac{1}{2}ab &= n \end{cases}$$

admet une solution en nombres rationnels a, b, c.

Par exemple, 6 est congruent : c'est l'aire d'un triangle rectangle dont les mesures des côtés sont 3, 4 et 5. De même, 5 est également congruent, bien qu'il soit moins aisé de trouver un triangle rectangle qui le prouve [9]. Fermat a montré que 1 n'est pas congruent. Plus généralement cependant, le problème de trouver un algorithme qui, étant donné un entier n, décide si oui ou non, n est congruent reste ouvert de nos jours, même si la théorie des courbes elliptiques permet d'en donner une réponse conjecturale.

En effet, par des manipulations algébriques astucieuses, mais néanmoins élémentaires, on peut démontrer que l'entier n est congruent si et seulement s'il existe un point P à coordonnées (x, y) rationnelles avec $y \neq 0$ sur la courbe elliptique d'équation $y^2 = x^3 - n^2x$. De plus, cette interprétation permet, pour un nombre congruent n donné, de construire une infinité de triangles rectangles d'aire n à côtés de longueur rationnelle. Ainsi, pour $n = 5$, avec la loi $\oplus$ décrite ci-dessus et un logiciel de calcul formel [10] on trouve alors par exemple que les triplets de nombres rationnels (a, b, c) suivants conviennent :

$$\left(\tfrac{3}{2}, \tfrac{20}{3}, \tfrac{41}{6}\right), \quad \left(\tfrac{1519}{492}, \tfrac{4920}{1519}, \tfrac{3344161}{747348}\right), \quad \left(\tfrac{25353117}{3525434}, \tfrac{35254340}{25353117}, \tfrac{654686219104361}{89380740677778}\right).$$

À l'aide de la conjecture de Birch et Swinnerton-Dyer mentionnée ci-dessus, Jerrold Tunnell est parvenu en 1983 à reformuler en un critère élémentaire la condition pour un entier d'être

8. Ce livre est également disponible en téléchargement gratuit (et légal) sur le site de l'auteur http://wstein.org/books/ent/.

9. Le lecteur que quelques tâtonnements infructueux auront rendu sceptique pourra facilement se convaincre que $a = 3/2$, $b = 20/3$ et $c = 41/6$ conviennent.

10. Par exemple le logiciel, libre et gratuit, Sage de W. Stein disponible à l'adresse http://www.sagemath.org/.

congruent, apportant ainsi une réponse conjecturale, mais extrêmement élégante, au problème mentionné plus haut.

La factorisation des grands entiers. On a déjà mentionné dans l'article *Mathématiques et secrets* de ce volume le système cryptographique RSA inventé en 1978 et encore très employé de nos jours. La sécurité de ce procédé repose fondamentalement sur l'extrême difficulté pratique à factoriser un « grand » entier [11]. Il y a quelques années, la société née de cette découverte avait d'ailleurs proposé, comme gage de la robustesse de ses produits, plusieurs défis consistant à décomposer certains entiers N donnés dont on savait qu'ils étaient le produit de seulement deux nombres premiers p et q. Le dernier à avoir été relevé date de 2009 et portait sur un entier N de 232 chiffres (une taille pourtant loin d'être déraisonnable). L'équipe qui y est parvenue était composée d'une douzaine de chercheurs et dans l'article (d'une vingtaine de pages) qui résume leur stratégie, les auteurs mentionnent que leurs calculs, s'ils avaient été menés sur un ordinateur personnel, auraient duré environ 2000 ans [12] !

Bien qu'indirecte et combinée à de nombreuses autres méthodes, l'utilisation de courbes elliptiques est désormais systématique dans ce genre de problèmes depuis que le mathématicien néerlandais Hendrik Lenstra [Len87] l'a introduite en 1987. Ses résultats, trop techniques pour être même résumés ici, ont cependant pour origine l'observation que la loi $\oplus$ définie ci-dessus se combine avec l'*arithmétique modulaire* (voir l'article de ce volume mentionné ci-dessus) pour produire une grande variété d'objets mathématiques (en fait de groupes finis) à partir desquels l'expérimentateur peut déceler les facteurs premiers d'un entier donné.

Références

[DMR76] Martin Davis, Yuri Matiyasevich, and Julia Robinson. Hilbert's tenth problem : Diophantine equations : positive aspects of a negative solution. In *Mathematical developments arising from Hilbert problems (Proc. Sympos. Pure Math., Vol. XXVIII, Northern Illinois Univ., De Kalb, Ill., 1974)*, pages 323–378. (loose erratum). Amer. Math. Soc., Providence, R. I., 1976.

[GG00] Ivor Grattan-Guinness. A sideways look at Hilbert's twenty-three problems of 1900. *Notices Amer. Math. Soc.*, 47(7) :752–757, 2000.

[Hen09] Guy Henniart. Congruent numbers, elliptic curves, and modular forms., 2009.

[Hil00] David Hilbert. Mathematical problems. *Bull. Amer. Math. Soc. (N.S.)*, 37(4) :407–436 (electronic), 2000. Reprinted from Bull. Amer. Math. Soc. **8** (1902), 437–479.

[Kna92] Anthony W Knapp. *Elliptic curves*, volume 40 of *Mathematical Notes*. Princeton University Press, Princeton, NJ, 1992.

[Len87] Hendrik W. Lenstra, Jr. Factoring integers with elliptic curves. *Ann. of Math. (2)*, 126(3) :649–673, 1987.

[Mat99] Yuri Matiyasevich. Le dixième problème de Hilbert : que peut-on faire avec les équations diophantiennes ? In *La recherche de la vérité*, Écrit. Math., pages 281–305. ACL-Éd. Kangourou, Paris, 1999.

11. On sait depuis Euclide que tout entier naturel ≥ 2 s'écrit (de façon unique à l'ordre près des facteurs) comme un produit de nombres premiers (c'est-à-dire de nombres divisibles seulement par 1 et par eux-mêmes). Le « jeu » consiste à les trouver dans la pratique.

12. Signalons au passage que la vérification de leur résultat (c'est-à-dire le calcul du produit de p par q) est d'une facilité déconcertante au regard de leurs efforts pour le trouver.

[Mor22] Louis Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. Cam. Phil. Soc.*, 21 :179, 1922.

[ST92] Joseph H. Silverman and John Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

[Ste09] William Stein. *Elementary number theory : primes, congruences, and secrets*. Undergraduate Texts in Mathematics. Springer, New York, 2009. A computational approach.

[Wil06] Andrew Wiles. The Birch and Swinnerton-Dyer conjecture. In *The millennium prize problems*, pages 31–41. Clay Math. Inst., Cambridge, MA, 2006.