CAHIERS DU SÉMINAIRE D'HISTOIRE DES MATHÉMATIQUES

CHRISTIAN HOUZEL

Introduction à l'histoire de l'analyse diophantienne

Cahiers du séminaire d'histoire des mathématiques 2^e série, tome 3 (1993), p. 1-12

<http://www.numdam.org/item?id=CSHM_1993_2_3__1_0>

INTRODUCTION A L'HISTOIRE DE L'ANALYSE DIOPHANTIENNE

Christian HOUZEL

L'analyse diophantienne est un sujet privilégié dans l'histoire des mathématiques; on peut la suivre depuis une antiquité reculée jusqu'à nos jours où elle est encore un sujet de recherches très actives, puisque les Babyloniens de la première dynastie (vers 1700 av. J.-C.) savaient en résoudre au moins un problème (triplets «pythagoriciens») et que l'un des résultats mathématiques les plus remarquables des dix dernières années se rapporte à ce secteur (Faltings 1983).

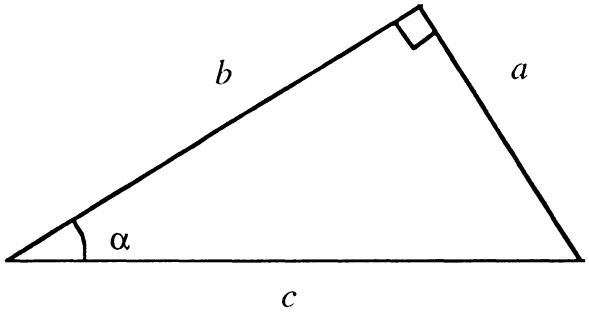
Dans la mathématique grecque, Diophante apparaît comme un phénomène assez isolé. Il a été lu et repris par les mathématiciens arabes du dixième siècle tantôt comme un algébriste (Al-Karajī), à la lumière de l'algèbre arabe qui se développait alors, tantôt comme un arithméticien (Al-Khāzin), à la lumière de l'arithmétique euclidienne des livres VII-IX. Sa redécouverte par Fermat au dix-septième siècle et les développements qu'il en a tirés marquent une date importante dans l'histoire des mathématiques; c'est la source de la théorie des nombres dans nos mathématiques actuelles. Elle s'est développée dans plusieurs directions, avec des liens multiples aux autres secteurs des mathématiques : formes quadratiques, calcul intégral et fonctions elliptiques, géométrie algébrique, approximations dites «diophantiennes» et nombres transcendants, logique (avec le dixième problème de Hilbert). Certains de ses problèmes anciens ne sont pas encore totalement résolus, comme celui des *nombres congruents* , le *dernier théorème de Fermat* ou la *conjecture de Catalan* .

On connaît Diophante d'Alexandrie à travers ses *Arithmétiques* composées en treize livres dont on a six en texte grec et quatre en traduction arabe, les trois autres étant perdus; on ne sait pas exactement à quelle époque il vivait, probablement au deuxième ou au troisième siècle de notre ère. La traduction arabe de Diophante date de la fin du neuvième siècle; dans la tradition latine, il a été redécouvert par divers auteurs comme Regiomontanus (XV^{e} siècle), Bombelli et Viète (XVI^{e} siècle) avant d'être publié par Xylander puis par Bachet de Méziriac (1621).

Triplets pythagoriciens et problèmes apparentés.

La première manifestation connue de l'analyse diophantienne se trouve dans une tablette cunéiforme de la première dynastie de Babylone. Il s'agit de la tablette n°322 dans la collection Plimpton conservée à l'Université Columbia de New York; elle a été publiée par

O. Neugebauer après la dernière guerre. Cette tablette comporte quinze lignes numérotées et trois colonnes de chiffres dont la dernière est en partie cassée. La première colonne donne l'*hypoténuse* (c), la deuxième un *côté* de l'angle droit (b) et la troisième le carré $\frac{c^2}{a^2} = \frac{1}{\sin^2\alpha}$



dans un triangle rectangle où α est l'angle adjacent à b ; les valeurs de α décroissent de 45° à 31° et la table est construite de manière que a ait des valeurs (sexagésimales) simples et que $\frac{c}{a}$ croisse en progression arithmétique. Ceci suppose que les Babyloniens de cette époque possédaient une méthode générale pour construire les triangles rectangles en nombres entiers, c'est-à-dire pour déterminer les *triplets pythagoriciens* (a,b,c) , formés de trois entiers liés par la relation $c^2 = a^2+b^2$.

Le problème des triplets pythagoriciens est justement le seul problème d'analyse indéterminée dont on trouve trace dans les *Éléments* d'Euclide, à la proposition 28 du livre X. Dans les *Arithmétiques* de Diophante, il correspond au problème 8 du livre II et c'est l'occasion de la célèbre observation marginale de Fermat, contenant l'énoncé du «dernier théorème». L'étude des triangles rectangles numériques est restée un des principaux sujets de recherche en analyse diophantienne; elle constitue le sujet même de l'analyse diophantienne *entière* pour Al-Khāzin (X^e siècle) qui rejetait l'analyse diophantienne *rationnelle* du côté de l'algèbre.

C'est dans ce contexte qu'Al-Khāzin pose le problème des *nombres congruents*, à la suite du problème 19 du livre III de Diophante; ce problème demande de trouver quatre nombres tels que le carré de leur somme augmenté ou diminué de chacun d'eux fasse un carré et comme, pour tout triplet pythagoricien (a,b,c) , $c^2 \pm 2ab = (a \pm b)^2$, Diophante se ramène à trouver quatre triangles rectangles numériques de même hypoténuse. Al-Khāzin se propose de trouver les nombres a pour lesquels il existe x tel que $x^2 \pm a$ soit un carré; il établit que a doit être le quadruple de l'aire d'un triangle rectangle numérique (comme dans le cas de Diophante) et il explicite l'identité $(a^2 + b^2)(\alpha^2 + \beta^2) = (a\,\alpha \mp b\,\beta)^2 + (a\,\beta \pm b\,\alpha)^2$ sous-jacente à la solution donnée par Diophante à son problème.

Ce problème se retrouve dans le *Livre des nombres carrés* de Léonard de Pise (1225), où on voit que, si x est entier, a est nécessairement divisible par 24 .

On appelle maintenant *nombre congruent* un entier $a \geq 1$ qui est l'aire d'un triangle rectangle à côtés rationnels; il revient au même de dire que l'équation $y^2 = x^3 - a^2x$ a une solution rationnelle (x,y) avec $y \neq 0$. A propos du problème 26 du livre VI de Diophante «trouver un triangle rectangle dont l'aire soit un nombre donné», Fermat démontre que l'aire d'un triangle rectangle ne peut pas être un carré; c'est le seul exemple explicite que l'on ait de lui pour la mise en œuvre de sa fameuse méthode de *descente infinie*. Il a ensuite établi qu'un nombre congruent n'est pas non plus le double d'un carré. Au dix-neuvième siècle Genocchi a trouvé des conditions nécessaires pour qu'un nombre soit congruent; par exemple il ne peut pas être un nombre premier de la forme $8k + 3$, ni le produit de deux nombres premiers distincts de cette forme, ni le double d'un nombre premier de la forme $8k + 5$, ni le double du produit de deux nombres premiers distincts de cette forme. On conjecture que les nombres de l'une des formes $8k + 5$, $8k + 6$ ou $8k + 7$ sont congruents; par exemple on sait que les nombres premiers de la forme $8k + 5$ ou $8k + 7$ sont congruents.

Le résultat de Fermat sur l'aire d'un triangle rectangle numérique implique l'impossibilité de $x^4 + y^4 = z^4$ c'est-à-dire un cas particulier du dernier théorème de Fermat. Diophante ne dit rien sur les problèmes *impossibles*, qui apparaissent dans la théorie des nombres chez les Arabes du dixième siècle, par exemple à propos de $x^3 + y^3 = z^3$ (autre cas du dernier théorème de Fermat); Al-Khujandī puis Al-Khāzin ont essayé sans succès de prouver l'impossibilité de cette équation. Au treizième siècle, Ibn al-Khawwān al-Baghdadī tente de démontrer que $x^4 + y^4 = z^4$ est impossible. Après Fermat, qui n'a jamais fait allusion publiquement à son «dernier théorème» pour d'autres exposants que 3 et 4 , Euler (1770) a publié une démonstration (par descente infinie) pour l'exposant 3 , fondée sur l'arithmétique des nombres de la forme $a + b\sqrt{-3}$ avec a et b entiers, dont Euler admet implicitement les propriétés qui lui sont nécessaires. D'autres exposants ont été abordés au dix-neuvième siècle : 5 (Dirichlet 1825), 14 (Dirichlet 1832), 7 (Lamé 1839); à la même époque, Sophie Germain a établi que, pour un exposant *premier* p tel que $2p+1$ soit aussi premier, l'équation de Fermat $x^p + y^p = z^p$ n'a pas de solution avec xyz non divisible par p («premier cas du théorème de Fermat») et Legendre a étendu ce résultat au cas où l'un des nombres $4p + 1$, $8p + 1$, $10p + 1$, $14p + 1$ ou $16p + 1$ est premier. Kummer (1846) a obtenu des résultats très remarquables au moyen de sa théorie des *corps cyclotomiques*, qui sont les corps $\mathbb{Q}(\zeta_p)$ où p est un nombre premier et ζ_p est une racine primitive p-ième de 1 ; il a pu établir que l'équation $x^p + y^p = z^p$ est impossible chaque fois que le nombre de classes d'idéaux de $\mathbb{Q}(\zeta_p)$ n'est pas divisible par p (on dit alors que p est *régulier*). Les nombres premiers inférieurs à 100 sont tous réguliers sauf 37 , 59 et 67 ; on ne sait toujours pas s'il existe une infinité de nombres premiers réguliers. À l'heure actuelle on sait démontrer le théorème pour les exposants inférieurs à 125000 et on sait que la «densité» des exposants pour lesquels il est vrai est égale à 1 (Heath-Brown); on sait que l'équation de Fermat pour un

exposant n donné ≥ 3 ne peut avoir qu'un nombre *fini* de solutions (Faltings) et que le premier cas est vrai pour une infinité d'exposants premiers (Fouvry).

L'Équation dite de Pell-Fermat.

Il s'agit, a étant un entier positif donné, non carré, de trouver x et y entiers tels que : $x^2 - ay^2 = \pm 1$. Ce genre de question apparaît dans la mathématique grecque à propos des approximations rationnelles de $\sqrt{a}$; pour $a = 2$, c'est la théorie des *nombres côtés* et des *nombres diamètres* à laquelle Platon fait allusion dans la *République* (II27.11-22) et que l'on connaît par Théon de Smyrne et par le commentaire de Proclus à la *République*. Les Grecs avaient un procédé récurrent pour construire une infinité de solutions (x,y) pour l'équation $x^2 - 2y^2 = \pm 1$ [de sorte que $(\frac{x}{y})^2 - 2 = \pm \frac{1}{y^2}$ et que $\frac{x}{y}$ donne une approximation de $\sqrt{2}$ d'autant meilleure que y est plus grand]; partant de $a_1 = d_1 = 1$, on pose, pour tout n,

$$a_n = 2a_{n-1} + d_{n-1} \quad , \quad d_n = a_{n-1} + d_{n-1}$$

et on voit que $d_n^2 - 2a_n^2 = \pm 1$. Les fractions ainsi obtenues sont des réduites du développement de $\sqrt{2}$ en fraction continue.

Le problème des *bœufs du Soleil*, attribué à Archimède, comporte un autre exemple d'équation de Pell-Fermat. La première partie du problème s'exprime par un système de 7 équations linéaires à 8 inconnues; la seconde impose des conditions arithmétiques sur deux sommes de deux inconnues (l'une doit être un carré, l'autre un nombre triangulaire) et, par élimination, on est conduit à l'équation $t^2 - 4729494u^2 = 1$, du type de Pell-Fermat.

Le *Brāhmasphuṭa-Siddhānta* de Brahmagupta (VII^e siècle) contient l'équation de Pell-Fermat ainsi que le *Bija-Ganita* de Bhāskara (XII^e siècle) avec une méthode de résolution cyclique (*cakravāla*) apparentée à l'algorithme d'Euclide. Le même genre de méthode servait à Brahmagupta, pour résoudre des problèmes indéterminés du *premier degré* (*kuṭṭaka*); en Chine, dès le cinquième siècle (Zhang Qiu-jian), une méthode analogue (*dayan*) était pratiquée. Le problème typique est celui des *100 volailles*, qui s'écrit comme le système diophantien

$$x + y + z = 100 \quad , \quad ax + by + cz = 100$$

(a, b, c coefficients donnés) et qui se ramène à une équation $\alpha x + \beta y = \gamma$; on le trouve mentionné dans le manuscrit d'une œuvre d'Alcuin (VIII^e siècle). Ce problème est traité complètement par Bachet de Méziriac dans ses *Problèmes plaisans et délectables* (1612); il est apparenté au problème des restes (théorème chinois).

Fermat avait proposé le problème dit maintenant de «Pell-Fermat» en défi aux mathématiciens anglais (1657); Brouncker et Wallis en ont proposé une solution assez analogue à la méthode indienne, mais ils ne prouvaient pas que leur algorithme conduisait toujours à une solution, ce que Fermat savait faire par descente infinie. Le problème a été étudié par Euler en liaison avec les équations diophantiennes du second degré, et c'est Euler

qui l'a faussement attribué au mathématicien anglais Pell. Lagrange est finalement parvenu à établir l'existence d'une solution dans tous les cas (1768), comme conséquence de son théorème sur la *périodicité* du développement en fraction continue d'un nombre quadratique.

Euler savait construire une infinité de solutions pour l'équation de Pell-Fermat en utilisant l'identité (*theorema eximium*)

$$\alpha(bc \pm ad)^2 - (bd \pm \alpha ac)^2 = (\alpha a^2 - b^2)(\alpha c^2 - d^2) \quad ;$$

ce genre d'identité est lié à la théorie des *formes quadratiques binaires*, comme $x^2 + y^2$, $x^2 \pm 2y^2$ ou $x^2 + 3y^2$ qu'Euler avait activement étudiées à la suite de Fermat. Le problème principal était de savoir quels nombres entiers étaient représentables par une telle forme; Lagrange a systématisé ces recherches (1773) en considérant les formes les plus générales

$$ax^2 + bxy + cy^2$$

et en introduisant les notions de *substitution linéaire*, d'*équivalence* des formes relativement à ces substitutions, de *formes réduites* et de *composition* des formes. Le travail de Lagrange est la base de la théorie développée par Gauss dans la cinquième section de ses *Disquisitiones arithmeticae* (1801).

Fermat énonce quels sont les nombres premiers qui s'écrivent sous la forme $x^2 + y^2$ en marge du problème III19 de Diophante: ce sont ceux qui sont de la forme $4k + 1$. Euler (1752) est parvenu a établir ce résultat de Fermat. A. Girard le connaissait d'ailleurs avant Fermat puisque, dans son édition des œuvres de S. Stevin (1634) il l'énonce à propos du problème V9 de Diophante: diviser l'unité en deux parties dont chacune, ajoutée à même nombre fixé, donne un carré. Si a est le nombre fixé, $2a + 1$ est une somme de deux carrés et Diophante avait déjà observé qu'une telle somme ne peut pas être de la forme $4k - 1$. Fermat énonce aussi (en marge du problème IV29 de Diophante) que tout nombre entier est la somme d'au plus 4 carrés entiers; Bachet l'avait vérifié empiriquement jusqu'à 325 (à propos du même problème diophantien). Euler a pu établir que tout entier est la somme de 4 carrés rationnels, laissant à Lagrange la gloire d'établir complètement le résultat de Fermat (1770).

Liens avec la géométrie algébrique.

Dans une note manuscrite de 1670, Newton interprète l'équation diophantienne $y^2 = P(x)$ où P est un polynôme de degré 3 comme la recherche des points à coordonnées rationnelles sur la cubique plane définie par cette équation (*Math. Pap.*IV, p.110-115). Mais ni Fermat, ni Euler, ni Lagrange ne s'expriment dans ce langage. Pourtant l'intérêt des méthodes diophantiennes pour trouver des changements de variable rendant rationnelle une forme différentielle à intégrer n'avait pas échappé à Leibniz ni à Daniel Bernoulli. Euler ramène certaines équations diophantiennes du quatrième degré à une forme canonique $\Phi(x,y) = 0$ (Φ polynôme de degré 2 en x et de degré 2 en y) qui lui permet d'obtenir une infinité de solutions; ses calculs sont identiques à ceux qu'il avait faits pour établir son théorème

d'addition des intégrales elliptiques mais il ne dit rien à ce sujet. Dans une note de 1834, Jacobi interprète la méthode d'Euler pour l'équation $y^2 = P(x)$ (P polynôme de degré 4) au moyen de la multiplication par n des intégrales elliptiques.

L'idée géométrique de Newton n'a été systématiquement reprise que vers la fin du dix-neuvième siècle dans des travaux de Sylvester (1858), Hilbert et Hurwitz (1890) et surtout Poincaré (1901). Or cette idée éclaire la lecture de Diophante beaucoup plus que la lecture algébrique qu'on en fait traditionnellement; elle permet mieux en effet de saisir le caractère systématique des méthodes diophantiennes tel que l'exprime d'ailleurs d'Alembert : «l'art de résoudre ces sortes de questions consiste à employer & à manier tellement les inconnues ou l'inconnue, que le quarré & les plus hautes puissances de cette inconnue disparoissent de l'équation, & qu'il ne reste que l'inconnue élevée au premier degré, au moyen de quoi on résout cette équation sans avoir recours aux incommensurables» (*Encyclopédie*, art. Diophante).

Illustrons ceci par l'exemple du problème 8 du livre II de Diophante où on demande de décomposer un carré, par exemple 16 , en somme de deux carrés; la méthode de Diophante consiste à prendre l'un des carrés comme carré d'une inconnue x^2 et à chercher l'autre carré sous la forme $y^2 = (mx - 4)^2 = m^2x^2 - 8mx + 16$, ce qui conduit à l'équation

$$(m^2 + 1)x^2 - 8mx = 0 \quad \text{d'où} \quad x = \frac{8m}{m^2 + 1} \quad \text{et} \quad y = 4\frac{m^2 - 1}{m^2 + 1}$$

(il faut que m soit rationnel et > 1 pour que $y > 0$ et Diophante prend d'emblée $m = 2$). Euler procède de même pour l'équation plus générale

$$(*) \qquad \alpha x^2 + \beta x + \gamma = y^2$$

dont il suppose connue une solution rationnelle (ou même entière) (a,b) ; il pose $x = a + mz$, $y = b + nz$ où z est une nouvelle inconnue (m, n paramètres rationnels) et il trouve $z = \dfrac{2\alpha am - 2bn + \beta m}{n^2 - \alpha m^2}$, d'où toutes les solutions rationnelles en faisant varier m et n.

Pour avoir les solutions *entières*, Euler est conduit à prendre m et n tels que $n^2 - \alpha m^2 = \pm 1$ (équation de Pell-Fermat). Ce procédé s'interprète géométriquement en remarquant que, pour (m,n) fixé et z variable, $(a + mz, b + nz)$ décrit une droite passant par le point (a,b) de l'hyperbole d'équation (*) ; la valeur cherchée de z correspond au deuxième point d'intersection de cette droite avec l'hyperbole et elle est donnée rationnellement car ce point est unique. La même méthode s'applique plus généralement à toute équation diophantienne du second degré $f(x,y) = 0$, qui s'interprète comme l'équation d'une conique; si (a,b) est une solution, on cherche les autres sous la forme $(a + mz, b + nz)$ et on trouve z par une équation de degré 1 ; c'est ce que fait Euler (1773).

Cette méthode, dite «de la corde», s'étend en degrés supérieurs grâce au théorème de Bézout (1764) d'après lequel deux courbes algébriques planes de degrés respectifs m et n ont

mn points d'intersection; plus précisément, si $f(x,y) = 0$ et $g(x,y) = 0$ sont des équations polynomiales de degrés respectifs m et n, l'équation en x obtenue en éliminant y est de degré mn. Si f est fixé et g variable (à coefficients rationnels) de manière que mn -1 des points d'intersection forment un «groupe rationnel», c'est-à-dire soient donnés par une équation de degré mn - 1 à coefficients rationnels, le dernier point d'intersection est donné rationnellement; par exemple pour $m = 3$ (cubique) et $n = 1$ (droite) on voit que la corde qui joint deux points rationnels d'une cubique recoupe cette courbe en un point rationnel et qu'il en est de même pour la tangente à la cubique en un point rationnel. Si la cubique possède un point double (nécessairement rationnel), une droite passant par ce point recoupe la courbe en un point rationnel et on obtient ainsi un paramétrage rationnel de la courbe.

Pour $m = 4$ (quartique) et $n = 2$ (conique), on voit qu'une conique ayant 7 points rationnels communs avec une quartique recoupe cette courbe en un point rationnel. Euler (1770) applique cette méthode pour trouver des solutions de $y^2 = A^2x^4 + 2Bx^3 + Cx^2 + 2Dx + E^2$, équation d'une quartique qui a deux branches tangentes à la droite de l'infini $t = 0$ au point $x = t = 0$; comme la parabole $y = ax^2 + bx + c$ est aussi tangente à $t = 0$ en ce point, elle a 4 points rationnels communs (à l'infini) avec la quartique et on peut choisir a, b et c de manière qu'elle en ait 3 de plus [la multiplicité du point commun à l'infini monte à 5 si $a = A$, à 6 si $b = \frac{B}{A}$ et à 7 si $c = \frac{C}{2A} - \frac{B^2}{2A^3}$ d'où un 8e point rationnel pour lequel $x = \frac{(B^2 - A^2C)^2 - 4A^6E^2}{4A^2(B(B^2 - A^2C) + 2A^4D)}$; une autre solution, donnée par Euler, consiste à utiliser le point rationnel $(0,E)$ à distance finie, par lequel passe la parabole si $c = E$, avec un contact d'ordre 2 si $b = \frac{D}{E}$ et d'ordre 3 si $a = \frac{C}{2E} - \frac{D^2}{2E^3}$].

Dans le cas d'une strophoïde $y^2(1 - x) = x^2(1 + x)$, qui a un point double à l'origine, on fait passer une droite $y = \xi x$ par ce point et on trouve $x = \frac{\xi^2 - 1}{\xi^2 + 1}$; inversement, $\xi = \frac{y}{x}$ de sorte que l'on a défini une *correspondance birationnelle* entre la strophoïde et la droite projective parcourue par ξ. Pour une cubique sans point singulier $f(x,y) = 0$ possédant un point rationnel P, on obtient un nouveau point rationnel $P' = (a,b)$ en recoupant par la tangente en P ; la droite $x = a + Xz$, $y = b + Yz$ (X,Y paramètres fixés) recoupe la cubique en 2 points donnés par l'équa-tion du second degré $\frac{1}{z} f(a + Xz, b + Yz) = Az^2 + Bz + C = 0$ où A, B et C sont des polynômes homogènes en X et Y, de degrés respectifs 3 , 2 et 1 . Pour la tangente en P, correspondant à $X = X_0$ et $Y = Y_0$, il y a une racine double c'est-à-dire que le polynôme $D = B^2 - AC$, homogène de degré 4 , s'annule en (X_0,Y_0) ; on peut choisir (X_0,Y_0) comme point à l'infini sur la droite projective parcourue par (X,Y) en faisant $X = X_0\xi + 1$, $Y = Y_0\xi$ et alors D devient un polynôme de degré 3 en ξ . Si $\eta^2 = D(\xi)$, on

résout l'équation en z par $z = \frac{-B + \eta}{A}$, d'où $x = a + z(X_0\xi + 1)$ et $y = b + zY_0\xi$ rationnellement en fonction de (ξ,η) ; inversement $\frac{1}{\xi} = \frac{x - a}{y - b} Y_0 - X_0$ et $z = x - a - \frac{X_0}{Y_0}(y - b)$ donc ξ et η sont rationnels en x et y. On établit ainsi une correspondance rationnelle entre la cubique et la courbe $\eta^2 = D(\xi)$ qui peut se ramener à la forme canonique de Weierstrass $\eta^2 = 4\xi^3 - g_2\xi - g_3$.

Une quartique $y^2 = P(x)$ (P polynôme de degré 4) avec un point rationnel connu peut se ramener à la même forme par équivalence birationnelle; on peut supposer que le point rationnel est donné par $x = 0$ de sorte que $P(0)$ est un carré. Un changement de variables $x' = \frac{1}{x}$, $y' = \frac{y}{x^2}$ envoie ce point à l'infini et on peut donc supposer que le coefficient dominant de P est un carré, ou même qu'il vaut 1 ; on est donc ramené à une équation $y^2 = x^4 - 6cx^2 + 4dx + e$ (où on a fait disparaître le terme en x^3 par une translation sur x). La parabole $y = x^2 + \xi$ a 6 points communs à l'infini avec cette quartique et deux points variables avec le paramètre ξ, donnés par l'équation $2(\xi + 3c)x^2 - 4dx + \xi^2 - e = 0$ dont le discriminant est $Q(\xi) = 4d^2 - 2(\xi + 3c)(\xi^2 - e)$ (polynôme de degré 3 en ξ); en posant $\eta^2 = Q(\xi)$ on a $x = \frac{2d + \eta}{2(\xi + 3c)}$, donc (x,y) rationnel en (ξ,η) et, inversement $\xi = y - x^2$, $\eta = 2x(y - x^2 + 3c) - 2d$.

On retrouve la même réduction pour la «double équation» déjà considérée par Diophante: $u^2 = Ax^2 + Bx + C$, $v^2 = A'x^2 + B'x + C'$, qui définit une biquadratique gauche, intersection de deux cylindres quadratiques. Si un point rationnel est connu, on peut l'envoyer à l'infini par une transformation homographique, de sorte que A et A' sont des carrés et on peut les supposer égaux à 1 ; par soustraction $u^2 - v^2 = (B - B')x + C - C'$ que l'on prend comme nouvelle inconnue x' (en supposant $B \neq B'$). Le système devient $u^2 - v^2 = x'$, $u^2 = a^2x'^2 + bx' + c$ (a,b,c rationnels) intersection d'un paraboloïde hyperbolique et d'un cylindre; on coupe par le plan $u + v = \xi$, tangent à l'infini au paraboloïde, d'où $u - v = \frac{x'}{\xi}$ puis $u = \frac{1}{2}(\xi + \frac{x'}{\xi})$, $v = \frac{1}{2}(\xi - \frac{x'}{\xi})$. L'inconnue x' est alors donnée par une équation de degré 2 dont le discriminant est

$$(\frac{1}{2} - b)^2 - (\xi^2 - 4c)(\frac{1}{4\xi^2} - a^2) = \frac{1}{\xi^2}[a^2\xi^4 + (b^2 - b - 4a^2c)\xi^2 + c] = \frac{\eta^2}{\xi^2} ;$$

ainsi $x' = \xi \frac{(2b - 1)\xi + 2\eta}{1 - 4a^2\xi^2}$, donc x', u et v sont donnés rationnellement en fonction de (ξ,η) et inversement $\xi = u + v$, $\eta = \frac{1}{2}[\frac{x'}{\xi}(1 - 4a^2\xi^2) - (2b - 1)\xi]$ de sorte que la biquadratique est birationnellement équivalente à la quartique plane $\eta^2 = a^2\xi^4 + (b^2 - b - 4a^2c)\xi^2 + c$. Par exemple le problème 13 du troisième livre de Diophante s'écrit comme la double équation

$$u^2 = 4x^2 + 15x \quad , \quad v^2 = 4x^2 - x - 4 \ ;$$

on a $u^2 - v^2 = 16x + 4 = 4x'$ avec $x' = 4x + 1$, $u = \xi + \frac{x'}{\xi}$, $v = \xi - \frac{x'}{\xi}$ et $u^2 = \frac{1}{4}(x'^2 + 13x' - 14)$ soit $(\frac{4}{\xi^2} - 1)x'^2 - 5x' + 4\xi^2 + 14 = 0$. Le discriminant de cette équation est $25 - 4(4\xi^2 + 14)(\frac{4}{\xi^2} - 1) = \frac{1}{\xi^2}(16\xi^4 + 17\xi - 224)$ et on pose $\eta^2 = 16\xi^4 + 17\xi^2 - 224$, équation équivalente à la double équation proposée; elle a une solution évidente $\xi = 2$, $\eta = -5$ qui donne $x' = 6$, $x = \frac{5}{4}$, $u = 5$ et $v = 1$.

Considérons maintenant une courbe plane irréductible C de degré n et d'équation $f(x,y) = 0$ à coefficients rationnels, avec d points doubles. On recherche ses points rationnels en considérant une courbe auxiliaire Γ de degré $n - 2$ à coefficients rationnels et qui passe par les d points doubles (ils forment un groupe rationnel; Γ est dite courbe *adjointe*); elle dépend de $\frac{n(n-1)}{2} - 1 - d = \frac{(n-2)(n+1)}{2} - d$ paramètres que l'on fixe en imposant à Γ de passer par un nombre égal de points de C . D'après le théorème de Bézout, une telle condition n'est possible que si

$$2d + \frac{(n-2)(n+1)}{2} - d = d + \frac{(n-2)(n+1)}{2} \leq n(n-2)$$

soit $d \leq \frac{(n-1)(n-2)}{2}$; alors Γ recoupe C en $p = \frac{(n-1)(n-2)}{2} - d$ points variables (et les points fixés sont en nombre $n - 2 + p$) . On dit que p est le *genre* de C ; l'importance du genre en analyse diophantienne provient de son invariance birationnelle.

Hilbert et Hurwitz (1890) ont établi qu'une courbe de genre 0 est birationnellement équivalente (par une transformation à coefficients rationnels) à une droite projective ou à une conique: un système rationnel de $n - 2$ points ordinaires de C détermine une courbe Γ qui ne recoupe C en aucun point variable; si $\varphi_j = 0$ $(1 \leq j \leq n - 1)$ sont les équations de $n - 1$ courbes adjointes indépendantes de degré $n - 2$, l'équation générale de Γ s'écrit $a_1\varphi_1 + a_2\varphi_2 + \ldots + a_{n-1}\varphi_{n-1} = 0$. Au point (x,y) de C on associe le point de coordonnées homogènes $(\varphi_j(x,y))$ dans l'espace projectif $\mathbb{P}_{n-2}$ et on transforme ainsi C en une courbe de

degré n -2 dans cet espace, birationnellement équivalente à C ; il suffit de recommencer pour abaisser encore le degré jusqu'à 1 ou 2 .

Poincaré (1901) s'est proposé de classer les problèmes diophantiens *modulo* les transformations birationnelles à coefficients rationnels et il a obtenu plusieurs résultats remarquables dans le cas du genre 1 en utili-sant systématiquement le paramétrage d'une courbe de genre 1 par des fonctions elliptiques. Une courbe C de degré $n \geq 4$ et de genre $p = 1$ doit avoir $\frac{n\,(n\,-\,3)}{2}$ points doubles. Supposons connu en outre un point ordinaire rationnel et soit X une courbe adjointe de degré n - 2 osculatrice à C en ce point; elle recoupe C en $n - 2 + 2p - 3 = n - 3$ points qui forment un système rationnel. On fait maintenant passer par ces n - 3 points une courbe adjointe Y de degré n - 2 ; elle dépend de $n - 2 + p - (n - 3) = 2$ paramètres et elle recoupe C en $n - 2 + 2p - (n - 3) = 3$ points variables qui forment un système rationnel. Si $\varphi_j = 0$ $(1 \leq j \leq 3)$ sont les équations de trois courbes Y indépendantes, l'équation générale s'écrit $a_1\varphi_1 + a_2\varphi_2 + a_3\varphi_3 = 0$; au point (x, y) de C on associe le point de $\mathbb{P}_2$ de coordonnées homogènes $(\varphi_j(x, y))$ et on établit ainsi une correspondance birationnelle entre C et une cubique plane, que l'on peut ramener à la forme de Weierstrass. Le paramétrage elliptique de la courbe de Weierstass $\xi = \wp u$, $\eta = \wp' u$ met en évidence la loi de groupe sur l'ensemble des points de la courbe car l'addition des paramètres u se fait par des formules rationnelles en ξ et η ; les points rationnels forment un sous-groupe G . Il semble que Poincaré admettait implicitement que le groupe G est de type fini; ce résultat a été obtenu par Mordell en 1922 au moyen de la descente infinie. Mordell établit d'abord, en se servant de l'arithmétique des nombres algébriques, que $G/2G$ est un groupe fini; un système de représentants S engendre donc un sous-groupe G_0 de type fini de G tel que $G = G_0 + 2G$. On a alors $G = G_0 + 2^{\nu}G$ pour tout entier ν , c'est-à-dire que tout point P s'écrit sous la forme $P_0 + 2^{\nu}Q$ où $P_0 \in G_0$ et $Q \in G$; Mordell démontre alors qu'il existe une constante M telle que, pour tout P on puisse trouver ν assez grand pour que la *hauteur* de Q soit majorée par M (la hauteur mesure la taille des coordonnées), d'où le fait que G est lui-même de type fini.

Mordell a conjecturé que les courbes de genre $p \geq 2$ ne pouvaient avoir qu'un nombre *fini* de points rationnels et Siegel (1926) est arrivé à démontrer qu'il n'y avait qu'un nombre fini de points *entiers* . A.Weil (1930) a essayé d'attaquer le problème au moyen du plongement de la courbe dans sa *jacobienne* , variété abélienne de dimension p sur laquelle on peut encore utiliser la loi de groupe; il est parvenu a établir que le groupe des points rationnels d'une variété abélienne est de type fini. C'est seulement en 1983 que G.Faltings a finalement démontré la conjecture de Mordell en utilisant tous les outils de la géométrie algébrique développés entre-temps.

Bibliographie

C.-G. BACHET de MEZIRIAC, *Problèmes plaisans et délectables qui se font par les nombres*, Lyon 1612; réimp. de la 5e éd., Paris, 1993.

H.T. COLEBROOKE, *Algebra with Arithmetic and Mensuration from the Sanskrit of Brahmegupta ans Bhaskara* , Londres, 1817.

L.E. DICKSON, *History of the Theory of Numbers* , Washington, 1919-1923; réimp. New York, Chelsea, 1971.

DIOPHANTE, *Les Arithmétiques* , éd.Allard et Rashed, Paris, 1984.

H. EDWARDS, *Fermat's Last Theorem* , New York ,1977.

L. EULER, *Opera*, ser.I, vol.1-6, Bâle, 1911-1944.

G. FALTINGS, Endlichkeitssätze für abelsche Varietaten über Zahlkörpern , *Inv. Math.*73 (1983), p.349-366.

P. de FERMAT, *Œuvres* , Paris, 1891-1896.

C.F. GAUSS, *Disquisitiones arithmeticae* , Leipzig, 1801 = *Werke* 1; trad. française Poullet-Delisle, Paris, 1807; réimp.1979.

T. HEATH, *Diophantus of Alexandria* , 2nd ed., New York, 1964.

C. HOUZEL, L'analyse diophantienne et la géométrie algébrique , *Encycl. Philos.*, Paris, 1988, t.1, p.1069-1075.

E.E. KUMMER, *Collected Papers* , New York, 1975, vol.1.

J.-L. LAGRANGE, *Œuvres* , vol.I (p.671-731), II (p.377-535 et 655-726), III (p.189-201 et 695-795) et VII (p.5-180), Paris, 1867-1892.

T.A. LAVRINENKO, Diofantovy uravnenija v rabotax L.Eilera, *Razvitije idei Leonarda Eilera i sovremennaja nauka*, Moscou (1988), p.153-165.

LÉONARD de Pise, *Liber quadratorum* , éd. Boncompagni, Rome, 1856; trad. française P.Ver Eecke, Bruges, 1952.

U. LIBBRECHT, The chinese Ta-Yen Rule , *Or. Lovan. Per.* 3 (1972), p.179-199.

L.J. MORDELL, *Three Lectures on Fermat's Last Theorem* , Cambridge, 1921; trad.française A.Sallin, Paris, 1929.

L.J. MORDELL, On the rational solutions of the indeterminate equations of the third and fourth degrees , *Proc.Cambridge Philos.Soc.*21 (1922), p.179-192.

L.J. MORDELL, *Diophantine equations* , New York, 1969.

O. NEUGEBAUER, *The exact Sciences in Antiquity* , New York, 1969

O. NEUGEBAUER et A. SACHS, *Mathematical cuneiform texts* , New Haven, 1945.

H. POINCARÉ, Sur les propriétés arithmétiques des courbes algébriques , *Journ.de Math.pures et appl.* V7 (1901), p.161-233 = *Œuvres* V, p.483-548.

R. RASHED, L'analyse diophantienne au X^{e} siècle: l'exemple d'al-Khāzin , *Rev.d'Hist.des Sciences* XXXII/3 (1979), p.193-222 = *Entre arithmétique et algèbre*, Paris, 1984, chap.IV1, p.195-225.

P. RIBENBOÏM, *13 Lectures on Fermat's Last Theorem* , New York, 1979.

A. WEIL, L'arithmétique sur les courbes algébriques, *Acta math.* 52 (1928), p.281-315.

A. WEIL, *Number theory, an approach through history from Hammurapi to Legendre* , Boston, 1983.