

rière de la table.

En 1989, Martin Bühler, à l'Université Yale, et Daniel Koditschek, à l'Université du Michigan, ont remplacé le dispositif de lancement circulant sur des rails par une barre en forme de boomerang, recouverte de velours. Pivotant autour d'un axe, chaque partie de cette barre frappe alternativement les palets. Pour contrôler la barre et obtenir ainsi une jonglerie permanente, les chercheurs ont utilisé ce qu'on appelle l'«algorithme miroir».

Cette machine utilise essentiellement deux idées. La première est de transformer la trajectoire continue du palet à l'aide d'une fonction non linéaire adéquate. Cela permet d'utiliser la connaissance imparfaite que l'on possède des caractéristiques (position, vitesse) du palet au point d'impact. La seconde est d'analyser l'énergie de la balle pour savoir si elle correspond à l'énergie d'un lancer parfait, afin de stabiliser le mouvement vertical du palet. Dès lors, le programme enregistre la position du palet, calcule la trajectoire de référence, ainsi que l'énergie réelle souhaitée pour le palet ; puis il calcule le moment où il faut frapper le palet et la force avec laquelle il faut le faire. Grâce à une version étendue de l'algorithme miroir, le robot exécute aussi une figure utilisant une seule main, avec deux palets et en deux dimensions. Il frappe le palet en ligne droite, alternativement avec les parties gauche et droite de la barre pivotante, dans deux colonnes séparées.

L'algorithme miroir donne des résultats impressionnants. Quand on perturbe l'un des palets, le bras du robot effectue des mouvements saccadés qui semblent artificiels aux yeux d'un jongleur humain, mais qui provoquent un retour rapide à une jonglerie normale. L'algorithme miroir commande efficacement la frappe du palet, mais ne s'étend pas au problème difficile qu'est la jonglerie avec des rattrapages contrôlés.

Outre la jonglerie par frappe et rebond, les robots parviennent à exécuter une foule d'activités liées à la jonglerie : faire valser des baguettes, faire sauter, projeter et attraper des balles dans une main en forme d'entonnoir et jouer une forme modifiée de ping-pong. Malgré tous ces progrès, aucun robot ne jongle d'une manière qui puisse ressembler, même



5. LE JONGLEUR PROFESSIONNEL Tony Duncan, dont les mains expertes apparaissent dans les clichés présentés ici, jongle également avec des massues.

vaguement, à la jonglerie humaine. Toutefois l'étude de la science de la jonglerie est récente, et les progrès réalisés au cours des 20 dernières années ont été remarquables. Il est possible que nous n'ayons pas à attendre longtemps avant de poser la devinette : «Comment le robot peut-il traverser le pont avec trois boulets de canon?»

Peter BEEK et Arthur LEWBEL peuvent jongler respectivement avec trois et huit balles. P. Beek est spécialiste de psychomotricité à l'Université libre d'Amsterdam. A. Lewbel a fondé le Club de jonglerie de l'Institut de technologie du Massachusetts et écrit dans la revue *Le monde de la jonglerie*.

Peter BEEK et Michael TURVEY, *Temporal Patterning in Cascade Juggling*, in *Journal of experimental Psychology*, vol. 18, n° 4, pp. 934-947, novembre 1992.

Scientific Aspects of Juggling, in *Claude Elwood Shannon : Collected Papers*, sous la direction de N.J.A. Sloane et A.D. Wyner, IEE Press, 1993.

J. BUHLER, D. EISENBUD, R. GRAHAM et C. WRIGHT, *Juggling Drops and Descents*, in *American Mathematical Monthly*, vol. 101, n° 6, pp. 507-519, juin-juillet 1994.

Tony van SANTVOORD et P. BEEK, *Phasing and the Pickup of Optical Information in Cascade Juggling*, in *Ecological Psychology*, vol. 6, n° 4, pp. 239-263, 1994.

Ian STEWART, *Juggling by Numbers*, in *New Scientist*, n° 1969, pp. 34-38, 18 mars 1995.

Service d'informations sur la jonglerie sur le serveur Web, à l'adresse : <http://www.hal.com/services/juggle/>

De Diophante à Fermat

CHRISTIAN HOUZEL

Le théorème de Fermat, récemment démontré, a son origine dans des problèmes qui datent du deuxième millénaire avant notre ère.

Sur son exemplaire des *Arithmétiques* de Diophante, en marge du problème 8 du livre II, le magistrat toulousain Pierre de Fermat écrit : «Au contraire, il est impossible de partager soit un cube en deux cubes, soit un bicarré en deux bicarrés, soit en général une puissance quelconque supérieure au carré en deux puissances de même degré ; j'en ai découvert une démonstration véritablement merveilleuse que cette marge est trop étroite pour contenir».

De nombreux mathématiciens ont cherché cette démonstration sans la trouver, jusqu'à ce que, en 1994, Andrew Wiles, de l'Institut Newton, à Cambridge, utilisant des outils mathématiques complètement inconnus du temps de Fermat, vienne à bout de ce que l'on a nommé «grand théorème de Fermat», alors qu'il ne s'agissait que d'une conjecture. Quelle preuve Fermat avait-il trouvée ? On l'ignore, et il y a peu de chances que les historiens des mathématiques parviennent jamais à le savoir. En revanche, on découvre encore des fragments de l'histoire du théorème de Fermat ; un autre article, de Yves Hellegouarch,

dans le prochain numéro de *Pour la Science*, montrera comment A. Wiles a résolu le problème.

Le problème 8 du livre II de Diophante était : «diviser un nombre carré en deux carrés». Cette équation qu'on noterait aujourd'hui $x^2 + y^2 = z^2$ est dite diophantienne, parce que l'on s'impose de trouver des nombres x, y, z qui soient rationnels, c'est-à-dire exprimables sous la forme de fractions. Les triplets (x, y, z) sont également nommés pythagoriciens, parce qu'ils peuvent être associés à des côtés de triangles

rectangles, qui vérifient alors le théorème de Pythagore.

Une tablette babylonienne

L'étude de tels «triangles rectangles en nombres», c'est-à-dire dont les côtés sont des nombres rationnels, était centrale dans l'analyse diophantienne traditionnelle ; elle remonte à une très haute antiquité, puisque une tablette babylonienne du début du II^e millénaire avant notre ère contient une table numérique visiblement liée aux triplets

pythagoriciens. Dans son état actuel (voir la figure 2), elle se compose de 15 lignes, numérotées de 1 à 15 dans la colonne de droite, avec trois autres colonnes ; des traces de colle, sur une cassure, dans la colonne de gauche, montrent qu'un morceau de la tablette a été perdu à l'époque moderne. Le titre de la première colonne n'est pas lisible, mais la deuxième colonne indique des «nombres de la largeur», la troisième colonne indique des «nombres de la diagonale», et la quatrième colonne donne un «nom».

Les nombres sont écrits en notation sexagésimale (chaque ordre valant soixante fois le précédent), sans indication de la position de la virgule, avec laquelle on sépare aujourd'hui les unités des chiffres



1. Pierre de Fermat, né en 1601 près de Toulouse, est le fondateur de la théorie des nombres. Fermat était magistrat, et il ne participa à la vie mathématique de son époque que par des correspondances privées avec d'autres savants.

décimaux (les Babyloniens se repéraient grâce au contexte). Par exemple, 1, 59, 0, 15 peut signifier $1 \times (59/60) + 0/(60 \times 60) + 15/(60 \times 60 \times 60)$, soit 1,9834...; 1,59 peut signifier $1 \times 60 + 59$, soit 119.

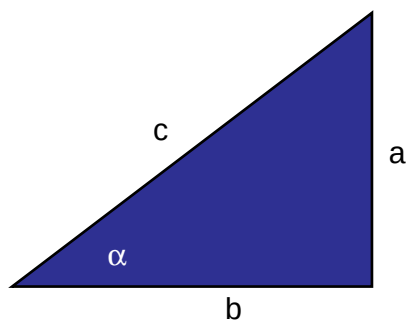
Sur le bas de la figure 2, on a reconstitué la première colonne, incomplète en raison de la cassure, en notant entre crochets les chiffres manquants ; les

nombres de cette colonne décroissent régulièrement de la première ligne ($1 + 59/60 + 15/60^3 = 1,9834...$ à la dernière ($1 + 23/60 + 13/60^2 + 46/60^3 + 40/60^4 = 1,387188...$). Cette décroissance s'éclaire si l'on interprète chaque nombre de la deuxième colonne comme un côté b de l'angle droit d'un triangle rectangle, et le nombre correspondant de la troisième colonne comme l'hypoténuse c ; le nombre associé, dans la première colonne, est alors le rapport c^2/a^2 , encore égal à $1/\sin^2\alpha$, où a est l'autre côté de l'angle droit et α l'angle opposé au côté de longueur a .

Cette tablette comporte quelques erreurs indiquées en couleur sur la figure, mais elle est remarquable : les valeurs du côté a (non indiquées dans la table) sont toutes des nombres entiers



2. CETTE TABLETTE BABYLONNIENNE mentionne des triplets pythagoriciens, c'est-à-dire qui peuvent être des longueurs de côtés de triangles rectangles. La notation est sexagésimale. Certains chiffres manquants sont indiqués entre crochets. La deuxième colonne contient des valeurs qui sont des côtés b de l'angle droit, la troisième colonne contient des valeurs de l'hypoténuse c et la première colonne contient des rapports c^2/a^2 , où a est l'autre côté de l'angle droit.



I	II	III	IV
[1,59,0,]15	1,59	2,49	1
[1,56,56,]58,14,50,6,15	56,7	3,12,1	2
[1,55,7,]41,15,33,45	1,16,41	1,50,49	3
[1,]5[3,1]0,29,32,52,16	3,31,49	5,9,1	4
[1,]48,54,1,40	1,5	1,37	5
[1,]47,6,41,40	5,19	8,1	6
[1,]43,11,56,28,26,40	38,11	59,1	7
[1,]41,33,59,3,45	13,19	20,49	8
[1,]38, 33,59,3,45	9,1	12,49	9
1,35,10,2,28,27,34,26,40	1,22,41	2,16,1	10
1,33,45	45	1,15	11
1,29,21,54,2,15	27,59	48,49	12
[1,]27,0,3,45	7,12,1	4,49	13
1,25,48,51,35,6,40	29,31	53,49	14
[1,]23,13,46,40	56	53	15

dont 2, 3, 5 sont les seuls facteurs premiers, de sorte que leurs inverses ont des expressions sexagésimales exactes : on peut donc penser que les Babyloniens disposaient d'une méthode systématique pour obtenir des triangles rectangles en nombres entiers, analogue à nos formules $a = 2pq$, $b = p^2 - q^2$ et $c = p^2 + q^2$ (la première ligne serait donnée par $p = 12$, $q = 5$, etc.). Le triangle de la onzième ligne a ses côtés (60, 45, 75) proportionnels au triplet pythagoricien le plus simple (4, 3, 5).

Certains historiens ont prétendu que les Égyptiens connaissaient ce triplet avant les Babyloniens. Ils n'en ont pas laissé de preuves. En revanche, on sait que les mathématiciens indiens, entre le V^e et le II^e siècle avant notre ère, étaient familiers de ces triplets : le texte des *Çulbasûtra* mentionne explicitement que les triplets (4, 3, 5), (12, 5, 13), (8, 15, 17), (24, 7, 25), (12, 35, 37) étaient utilisés pour construire des rectangles.

Les études de Diophante

La construction des triplets pythagoriciens est le seul résultat d'analyse diophantienne (avant Diophante) présent dans les *Éléments* d'Euclide (vers 300 avant notre ère) : c'est un lemme, ou résultat préalable, pour la proposition 28 du livre X. Le cas particulier où q est égal à $p - 1$ est d'ailleurs attribué par le philosophe Proclus à Pythagore (VI^e siècle avant notre ère) et celui où q est égal à 1 à Platon.

De combien le travail de Diophante est-il ultérieur ? Nul ne sait exactement, car on ignore si ce mathématicien alexandrin vivait au II^e siècle de notre ère, ou plutôt au III^e siècle. Une épigramme de l'*Anthologie palatine*, recueil de poèmes parfois anonymes écrits dans les premiers siècles de notre ère, c'est-à-dire peu après la mort de Diophante, contient un problème d'arithmétique élémentaire qui met en scène sa vie. Le livre XIV de l'*Anthologie palatine* est constitué de devinettes et de problèmes arithmétiques, dont certains sont indé-

terminés, mais très simples, tandis que Diophante, avec ses problèmes très difficiles, est un auteur isolé dans la mathématique grecque : le seul problème diophantien difficile connu en dehors des œuvres de Diophante est le problème des bœufs, attribué à Archimède, qui conduit à l'équation du type de Pell-Fermat : $t^2 - 4\,729u^2 = 1$ (ce problème concerne des bœufs qui paissent dans un pré ; exprimé sous forme d'un poème, il propose un système

Les *Arithmétiques* auraient été composées de 13 livres, mais on ne connaît que certains d'entre eux. Six sont connus par leur texte en grec, à travers de manuscrits dont les plus anciens remontent au XIII^e siècle ; quatre d'entre eux, dont l'original grec est perdu, ont été identifiés en 1971 par l'historien français des mathématiques Roshdi Rashed et publiés en 1984. Aujourd'hui on dispose donc de 10 des 13 livres : les trois premiers en grec (la

traduction arabe est perdue, mais on la connaît par des commentaires du X^e siècle), les quatre suivants en arabe, et les trois derniers en grec.

Dans les *Arithmétiques*, Diophante examine diverses espèces de nombres : les carrés, les cubes et les espèces que l'on obtient par combinaison des deux premières sortes (un carré-carré, par exemple, est un carré dont le côté serait un carré) ; il examine des problèmes où ces espèces sont combinées par addition, soustraction ou multiplication, de manière à donner des carrés ou des cubes. Les nombres considérés sont rationnels positifs (et pas seulement des entiers, comme dans la tradition euclidienne), et Diophante se ramène toujours, par des choix habiles, à ne conserver qu'un seul nombre inconnu, qu'il nomme simplement *arithmos*, c'est-à-dire «nombre», en grec. Il se contente généralement de trouver une solution pour chaque problème. Par exemple, pour le problème 8 du livre II, il cherche à diviser 16 en une somme de deux carrés, et il prend l'un de ces carrés inconnus comme carré du nombre (*dunamis*), soit x^2 ; l'autre carré est $16 - x^2$,

que Diophante cherche à évaluer au carré «d'un nombre quelconque d'*arithmos* diminué d'autant d'unités qu'il y a dans le côté de 16», par exemple à $(2x - 4)^2$, ce qui donne l'équation $5x^2 = 16x$, d'où $x = 16/5$.

Les manipulations de Diophante conduisent à ne conserver qu'une espèce égalée à une espèce : comme le dit d'Alembert (à l'article «Diophante» de l'*Encyclopédie*), il s'agit de «manier



3. L'ARITHMÉTIQUE fut rédigée par Diophante au II^e ou au III^e siècle de notre ère. Elle semble avoir été composée de 13 livres, dont seulement dix sont en notre possession : six sont en grecs et quatre sont en arabe. En marge de ce texte, Fermat écrivit avoir trouvé une solution merveilleuse qui n'a jamais été retrouvée.

de sept équations à huit inconnues avec quelques conditions).

On connaît de Diophante une œuvre intitulée *Les Arithmétiques* et un opuscule sur les nombres polygonaux, c'est-à-dire représentables par des sommets de polygones (par exemple, les carrés sont les nombres carrés, que l'on peut associer aux nombres de sommets de carrés emboîtés de plus en plus grands) ; on lui attribue également des *Porismes* aujourd'hui perdus.

tellement les inconnues ou l'inconnue, que le carré et les plus hautes puissances de cette inconnue disparaissent, et qu'il ne reste que l'inconnue au premier degré».

Les problèmes qui se rattachent aux triangles rectangles en nombres rationnels sont nombreux dans les *Arithmétiques*. Tantôt ces triangles interviennent comme auxiliaires pour résoudre un autre problème, comme dans le cas du problème 9 du livre III : «trouver quatre nombres tels que le carré de leur somme, augmenté ou diminué de n'importe lequel d'entre eux, fasse un carré». À propos de ce problème, Diophante observe que si $a^2 + b^2 = c^2$, alors $c^2 \pm 2ab = (a \pm b)^2$. Il cherche alors quatre triangles rectangles numériques (dont on note respectivement les deux côtés de l'angle droit $(a_1, b_1), (a_2, b_2), (a_3, b_3), (a_4, b_4)$) ayant la même hypoténuse c ; tous ces nombres doivent alors vérifier $c^2 = a_1^2 + b_1^2 = a_2^2 + b_2^2 = a_3^2 + b_3^2 = a_4^2 + b_4^2$. Il choisit habilement de chercher les quatre nombres sous la forme $2a_1b_1x^2, 2a_2b_2x^2, 2a_3b_3x^2, 2a_4b_4x^2$, où x est un nombre à déterminer, de façon que la somme des quatre nombres soit cx , ce qui donne $x = c/2(a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4)$. Il choisit c égal à 13×5 , soit 65, car il sait que le produit de deux sommes de deux carrés s'écrit de deux manières différentes comme une somme de deux carrés, et donc que 65^2 est somme de deux carrés de quatre manières.

Tantôt Diophante cherche plutôt des triangles rectangles numériques qui vérifient des conditions supplémentaires. Le livre VI, dans la numération grecque, est entièrement consacré à ce genre de problèmes. Par exemple, le problème 3 du livre VI demande de «trouver un triangle rectangle en nombres, dont l'aire, augmentée d'un nombre donné, fasse un carré». Le nombre donné est 5 ; Diophante cherche le triangle sous la forme (ax, bx, cx) , où (a, b, c) est un triplet pythagoricien, et le carré sous la forme $(mx)^2$; avec ce choix, la condition du problème devient $(m^2 - ab/2)x^2 = 5$. Il faut trouver a, b et m de manière que $m^2 - ab/2$ soit le cinquième d'un carré. Diophante trouve à nouveau un changement de variable astucieux : il prend $a = 2, b = p^2 - 1/p^2$ et $m = p + 2 \times 5/p$, ce qui conduit au problème auxiliaire : trouver p tel que $100p^2 + 505$ soit un carré. Ce problème est résolu comme le problème 8 du livre II, en posant $100p^2 + 505 = (10p + 5)^2$, d'où $p = 24/5$ et $1/5 \times (265/24)^2 x^2 = 5$, soit $x = 24/53$.

Les mathématiciens arabes

La traduction des *Arithmétiques* en arabe avait été suscitée par un intérêt croissant pour l'analyse indéterminée, à partir de la première moitié du IX^e siècle (dans les problèmes d'analyse indéterminée, on cherche à résoudre, en nombres rationnels, des systèmes d'équations qui ont plus d'inconnues que d'équations) ; le vocabulaire employé est emprunté à l'algèbre.

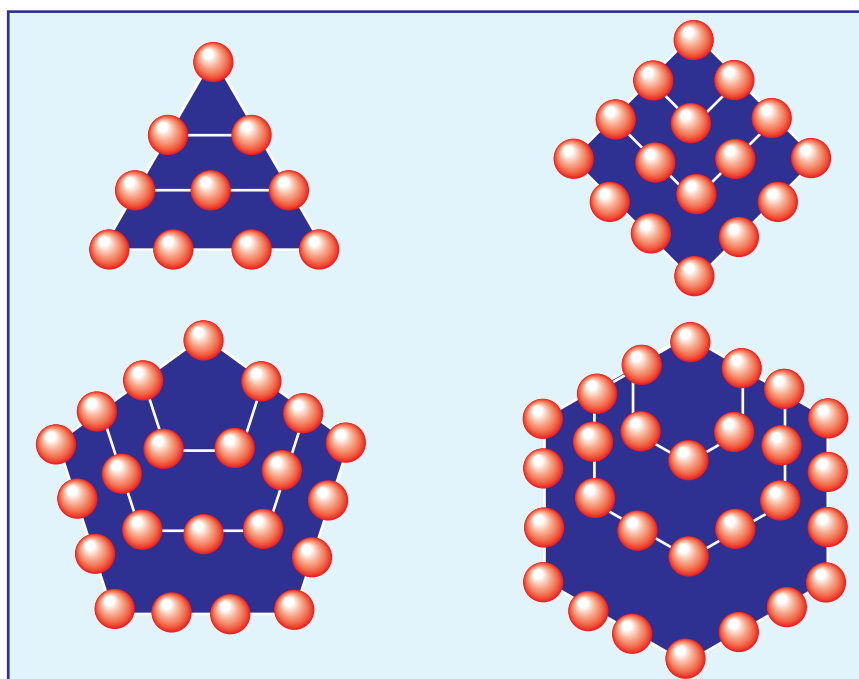
Cependant, à côté de cette lecture algébrique de Diophante, il s'est développé au X^e siècle une lecture plus proprement arithmétique, dont le représentant le plus éminent fut al-Khâzin. Cette tradition s'intéresse aux problèmes en nombres entiers, et pas seulement rationnels, et elle revient en cela à la représentation euclidienne des entiers par des segments de longueur multiples d'une longueur de base. Elle s'inscrit dans le cadre de la théorie des triangles rectangles en nombres entiers (avec le concept de triangle primitif, c'est-à-dire dont les longueurs des trois côtés n'ont pas de facteurs communs) et elle considère de nouveaux problèmes comme celui des nombres «congruents», que nous allons examiner, ainsi que des problèmes impossibles comme la division d'un cube en somme de deux cubes.

Le problème des nombres congruents est posé pour la première

fois dans un traité arabe anonyme, qui ne sera publié qu'en 1861 par l'historien des mathématiques F. Woepcke, et il a été repris par de nombreux mathématiciens. Dans la formulation d'al-Khâzin, il s'agit de «chercher un nombre carré tel que, si on lui ajoute un nombre donné et si on en retranche ce nombre donné, la somme et la différence soient deux carrés» (ce problème consiste à trouver trois nombres entiers x, y_1 et y_2 tels que $x^2 + a = y_1^2$ et $x^2 - a = y_2^2$).

Al-Khâzin se réfère au problème 19 du livre III de Diophante («trouver quatre nombres tels que le carré de leur somme, augmenté ou diminué de n'importe lequel d'entre eux, fasse un carré») ; par addition des deux équations, le double du carré cherché x^2 est somme de deux carrés $y_1^2 + y_2^2$. Une petite manipulation montre que ce carré est lui-même somme de deux carrés, $x^2 = u^2 + v^2$, où u et v sont respectivement la demi-somme et la demi-différence de y_1 et de y_2 . Alors $2uv$ est la demi-différence des deux carrés, c'est-à-dire le nombre donné a ; inversement, si $u^2 + v^2 = x^2$ et si $2uv = a$, en posant $y_1 = u + v$ et $y_2 = u - v$, on trouve $y_1^2 = x^2 + a$ et $y_2^2 = x^2 - a$.

Puisque les nombres x, u et v vérifient la relation de Pythagore, x est l'hypoténuse d'un triangle rectangle et a (égal à $2uv$) est quatre fois l'aire de ce triangle ; la plus petite valeur de a est



4. DIOPHANTE FUT L'AUTEUR d'un opuscule sur les nombres polygonaux, représentables par des sommets de polygones. Ici on a représenté des nombres triangulaires, des nombres carrés, des nombres pentagonaux et des nombres hexagonaux.

Si l'aire d'un triangle était un carré, il y aurait deux bicarrés dont la différence serait un carré; il s'ensuit qu'on aurait également deux carrés dont la somme et la différence seraient des carrés. Par conséquent, on aurait un nombre carré, somme d'un carré et du double d'un carré, avec la condition que la somme des deux carrés, qui servent à le composer, soit également un carré. Mais si un nombre carré est somme d'un carré et du double d'un carré, sa racine est également somme d'un carré et du double d'un carré, ce que je puis prouver sans difficulté. On conclura de là que cette racine est la somme des deux côtés de l'angle droit d'un triangle rectangle, dont l'un des carrés composants formera la base, et le double de l'autre carré la hauteur.

Ce triangle rectangle sera donc formé par deux nombres carrés, dont la somme et la différence seront des carrés. Mais on prouvera que la somme de ces deux carrés est plus petite que celle des deux premiers dont on a également supposé que la somme et la différence soient des carrés. Donc, si on donne deux carrés dont la somme et la différence soient des carrés, on donne par là même, en nombres entiers, deux carrés jouissant de la même propriété et dont la somme est inférieure.

Par le même raisonnement, on aura ensuite une autre somme plus petite que celle déduite de la première, et en continuant indéfiniment on trouvera toujours des nombres entiers de plus en plus petits satisfaisant aux mêmes conditions. Mais cela est impossible, puisqu'un nombre entier étant donné, il ne peut y avoir une infinité de nombres entiers qui soient plus petits.

La marge est trop étroite pour recevoir la démonstration complète et avec tous ses développements.

Par le même procédé, j'ai découvert et démontré qu'il n'y a aucun nombre triangulaire, sauf l'unité, qui soit un bicarré.

5. LE FILS DE PIERRE DE FERMAT a publié en 1670 les *Arithmétiques* de Diophante avec les annotations marginales de son père. Dans ces œuvres figure la mention du problème de Diophante et le texte où Fermat annonçait avoir résolu ce problème.

24 (on cherche des nombres tous différents), qui correspond au triplet pythagoricien le plus petit (4,3,5).

Al-Khâzin donne ensuite plusieurs méthodes relevant de l'algèbre pour résoudre le problème en nombres rationnels et non plus entiers; les nombres entiers a possibles sont dits congruents. Enfin il établit l'identité $(p^2 + q^2)(r^2 + s^2) = (pr + qs)^2 + (ps - qr)^2$, implicite dans le raisonnement de Diophante sur les nombres représentables de plusieurs manières, comme somme de carrés.

On retrouve cette identité dans le *Livre des nombres carrés* (1225) de Léonard de Pise, encore connu sous le nom de Fibonacci. Bien qu'écrit en latin, ce livre se rattache aux mathématiques arabes; il

est publié à l'occasion une question posée à Léonard de Pise par Jean de Palerme, à la cour de l'empereur Frédéric II: trouver un carré x^2 qui, augmenté et diminué de 5, donne toujours un carré. Léonard commence par l'étude générale du problème en nombres entiers, remplaçant 5 par un nombre entier a ; il établit tout d'abord que le nombre a doit s'écrire $4pq(p^2 - q^2)$ (c'est quatre fois l'aire d'un triangle rectangle), puis il montre que ce nombre est nécessairement un multiple de 24.

Pour obtenir un nombre égal à cinq fois un carré, il prend $p = 5$ et $q = 4$; il obtient alors $a = 720 = 12^2 \times 5$, $x = p^2 + q^2 = 41$, tel que $41^2 + 720 = 49^2$, et $41^2 - 720 = 31^2$, ce qui permet de résoudre

le problème de Jean de Palerme avec $x = 41/12$.

Les problèmes impossibles

Un certain al-Khujandî, au X^e siècle, aurait proposé une démonstration incorrecte du fait que «la somme de deux nombres cubiques n'est pas un cube»; on connaît un texte de cette époque, attribué à un Abû Ja'far (ce qui est d'ailleurs un des noms d'al-Khâzin), qui pourrait bien être cette tentative. L'auteur établit géométriquement que «pour deux nombres cubiques, leur différence est la somme du produit du carré du plus petit côté par la différence des deux côtés, plus le produit de la somme des deux côtés par leur différence, en ensuite par le plus grand côté». Autrement dit: $z^3 - y^3 = y^2(z - y) + (z + y)(z - y)z$. Puis, entraîné par le langage géométrique, il affirme péremptoirement que cette expression n'est pas un cube (au sens géométrique), ce qui n'est évidemment pas une démonstration.

Une liste de 33 problèmes impossibles considérés par Ibn al-Khawwâm al-Baghdâdî, à la fin du XIII^e siècle, est connue par le commentaire qu'en fait un élève, Kamâl al-Dîn al-Fârisî. Al-Baghdâdî écrit: «Nous ne prétendons pas que nous pouvons établir leur impossibilité, mais nous affirmons que nous ne pouvons pas les résoudre». Parmi ces problèmes, le premier s'énonce: «Trouver deux carrés dont la somme et la différence soient des carrés». Autrement dit, un carré ne pourrait pas être congruent. Le troisième problème est «trouver un triangle rectangle dont les côtés sont des carrés», et le 24-ième: «diviser un cube en deux cubes». Ce sont précisément les équations de Fermat pour les exposants 4 et 3.

Fermat, enfin

Diophante a été progressivement redécouvert en grec, dans le monde européen, à partir du XVI^e siècle. Le mathématicien italien Rafael Bombelli (1526-1572) a consulté un manuscrit des *Arithmétiques* à la bibliothèque du Vatican; puis l'érudit W. Holzmänn, qui signait Xylander, en a publié une traduction en latin en 1575. Enfin le Français Gaspard Bachet de Méziriac (1581-1638) a publié le texte grec avec un traduction latine en 1621, et c'est dans cette traduction que Fermat a pris

connaissance de Diophante. Dans les marges de son exemplaire personnel, il a mis un certain nombre d'observations, et son fils Samuel a publié en 1670 le texte de Diophante complété par les annotations paternelles. Ces observations sont une source d'informations précieuse pour la connaissance des travaux arithmétiques de Fermat.

Ce dernier, comme avant lui al-Khâzin, distingue entre l'analyse diophantienne en nombres entiers, dite arithmétique, et l'analyse diophantienne en nombres rationnels, plus algébrique et que Fermat rejette du côté de la géométrie, c'est-à-dire de la science des quantités continues. Dans un défi qu'il lance aux mathématiciens en 1657, il commence par ces mots : «Il est à peine quelqu'un qui propose des questions purement arithmétiques, il est à peine quelqu'un qui sache les résoudre. Est-ce parce que l'Arithmétique a plutôt été traitée jusqu'à présent au moyen de la Géométrie que par elle-même ? C'est la tendance qui apparaît dans la plupart des Ouvrages tant anciens que modernes et dans Diophante lui-même. Car s'il s'est écarté de la Géométrie un peu plus que les autres en astreignant son analyse à ne considérer que des nombres rationnels, il ne s'en est pas dégagé tout à fait, comme le prouvent surabondamment les *Zététiques* de Viète, dans lesquelles la méthode de Diophante est étendue à la quantité continue et, par suite, à la Géométrie». Contrairement à Diophante, Fermat cherche à déterminer toutes les solutions de chaque problème indéterminé.

Le principe unificateur de son analyse en nombres entiers semble être sa méthode de descente infinie : dans cette méthode, on part d'une solution en nombres entiers positifs d'une équation ; on en déduit qu'il existe alors une autre solution, en nombres entiers positifs, mais plus petits que les précédents ; puis en répétant cette construction sur la solution plus petite, on trouve une solution encore inférieure, et on répète indéfiniment le processus. Comme toutes les solutions ainsi obtenues sont des nombres entiers positifs et qu'il n'existe pas de suite infinie décroissante d'entiers positifs (on s'arrête évidemment à 0), l'équation ne peut avoir de solution.

Les principaux problèmes qu'il est parvenu à résoudre par cette méthode sont déjà énoncés dans une lettre au père Mersenne, au début

juin 1638 : trouver un triangle rectangle en nombres, dont l'aire soit un carré ; trouver deux carrés-carrés (deux puissances quatrièmes) dont la somme soit un carré-carré, ou deux cubes dont la somme soit un cube ; trouver trois carrés en progression arithmétique (avec le même écart entre le premier et le deuxième carré qu'entre le deuxième et le troisième) sous la condition que la différence de la progression soit un carré.

À ces problèmes, Fermat ajoute des théorèmes : (1) Tout nombre est somme d'un, de deux ou de trois «triangles» (c'est-à-dire nombres triangulaires ; voir la figure 4) ; d'un, deux, trois ou quatre carrés ; d'un, deux, trois, quatre ou cinq pentagones ; d'un, deux, trois, quatre, cinq ou six hexagones ; d'un, deux, trois, quatre, cinq, six ou sept heptagones, et ainsi de suite indéfiniment. (2) Un multiple de 8 diminué d'une unité se compose seulement de quatre carrés, non seulement en entiers, mais même en fractions». D'autres sont énoncés en août 1659 dans une lettre à Pierre de Carcavi, un magistrat parisien avec lequel Fermat correspondait.

On n'a que deux exemples de démonstrations par descente infinie de la main de Fermat : l'une se trouve en marge d'un problème ajouté par Bachet à la fin du livre VI de Diophante : «Trouver un triangle rectangle dont l'aire soit un nombre donné». Fermat ajoute : «L'aire d'un triangle rectangle en

nombres ne peut être un carré(...) Si l'aire d'un triangle était un carré, il y aurait deux bicarrés dont la différence serait un carré ; il s'ensuit qu'on aurait également deux carrés dont la somme et la différence seraient des carrés(...) Donc si on donne deux carrés dont la somme et la différence sont des carrés, on donne par là même, en nombres entiers, deux carrés jouissant de la même propriété et dont la somme est inférieure. Par le même raisonnement, on aura ensuite une autre somme plus petite que celle déduite de la première, et, en continuant indéfiniment, on trouvera toujours des nombres entiers de plus en plus petits satisfaisants aux mêmes conditions. Mais cela est impossible, puisqu'un nombre entier étant donné, il ne peut y avoir une infinité de nombres entiers qui soient plus petits...»

Traduisons algébriquement le discours de Fermat : pour le triangle rectangle de côtés de l'angle droit $2pq$, $p^2 - q^2$, et d'hypoténuse $p^2 + q^2$, l'aire $pq(p^2 - q^2)$ étant un carré, les nombres p , q , $p^2 - q^2$ sont des carrés, car p et q sont supposés premiers eux (ils n'ont pas de facteur commun) et de parités différentes (sinon le facteur 2 serait facteur commun) ; ainsi $p = u^2$, $q = v^2$ et $p^2 - q^2 = u^4 - v^4 = (u^2 + v^2)(u^2 - v^2)$ est un carré, donc $u^2 + v^2 = s^2$ et $u^2 - v^2 = t^2$. On déduit que $s^2 = t^2 + 2v^2$, et que $s = m^2 + 2n^2$, $t = m^2 - 2n^2$, et $v = 2mn$, de sorte que $u^2 = t^2 + v^2 = (m^2)^2 + (2n^2)^2$ et $(2n^2, m^2, u)$ est un nouveau triangle



6. LA MÉTHODE DE LA CORDE, inventée par Newton, fut appliquée à la fin du siècle dernier à des courbes d'équation $y^2 = P(x)$, où P est un polynôme de degré égal à trois. Newton a remarqué qu'une droite qui passe par deux points de coordonnées rationnelles de la courbe passe également par un troisième point rationnel. La méthode de la tangente correspond au cas particulier où deux points sont confondus : la sécante devient une tangente, de sorte qu'un point rationnel en détermine un autre.

rectangle dont l'aire m^2n^2 est un carré ; alors $m^2 = u_1^4 - v_1^4$, avec des nombres u_1, v_1 , tels que $u_1^2 \pm v_1^2$ soit carré, et on voit que $u_1^2 + v_1^2 < u^2 + v^2$. Cette démonstration donne l'impossibilité de l'équation de Fermat pour l'exposant 4.

Dans sa correspondance ou dans ses travaux publiés, Fermat n'a jamais fait allusion à son équation pour d'autres exposants que 3 et 4. Il est donc permis de penser qu'il s'est aperçu après coup d'une difficulté dans la démonstration qu'il croyait avoir pour le cas général de sa conjecture.

Les successeurs de Fermat

Pendant le XVII^e siècle, l'analyse diophantienne est restée un sujet à la mode qui a intéressé notamment Isaac Newton et Wilhelm von Leibniz. Au premier, on doit une note remarquable dans un cahier de 1670, où il interprète l'équation diophantienne $y^2 = P(x)$, où P est un polynôme de degré égal à trois (de la forme $ax^3 + bx^2 + cx + d$), comme la recherche des points à coordonnées rationnelles sur la courbe définie par cette équation. Newton explique comment une sécante qui joint deux points rationnels (c'est-à-dire dont l'abscisse et l'ordonnée sont des nombres rationnels) recoupe la courbe en un troisième point rationnel, mais cette interprétation par la géométrie algébrique reste isolée, à l'époque (voir la figure 6).

Leibniz avait découvert que certaines manipulations de l'analyse diophantienne conduisant à exprimer rationnellement, en fonction d'un paramètre, des quantités x et y liées par une relation algébrique $f(x,y) = 0$, pouvaient être employées pour obtenir des intégrales de y en fonction de x (l'aire sous la courbe donnée par l'équation $y = f(x)$). On trouve une remarque analogue dans des lettres du mathématicien suisse Daniel Bernoulli (1700-1782) à Christian Goldbach (1690-1764), en décembre 1723 et en mars 1724.

C'est précisément par Goldbach que l'attention du Bâlois Léonard Euler (1707-1783) a été attirée sur les travaux arithmétiques de Fermat, à partir de 1730. Euler a beaucoup étudié le grand théorème de Fermat, et beaucoup de ses travaux sont consacrés à des démonstrations de résultats annoncés par Fermat.

Le premier thème est l'étude des équations diophantiennes de degré

égal à deux. En supposant connue une solution rationnelle, il aborde la recherche des autres solutions d'une manière analogue à celle de Diophante pour le problème 8 du livre II, et il remarque que la détermination des solutions entières exige la résolution d'une équation du type de Pell-Fermat.

Un deuxième thème est l'étude des équations de la forme $y^2 = P(x)$, où P est un polynôme de degré égal à trois ou quatre, et des problèmes apparentés. On peut y rattacher l'impossibilité de l'équation $x^4 + y^4 = z^2$, qu'Euler établit, en 1747, par descente infinie, à la manière de Fermat, et dont il tire une série de corollaires.

Les constructions d'Euler relatives à ces équations peuvent s'interpréter géométriquement comme l'avait fait Newton (méthode de la sécante ou de la tangente), mais Euler n'en dit rien. Le lien avec le calcul intégral ne lui avait peut-être pas échappé, car, vers 1780, il transforme l'équation $y^2 = P(x)$ en une autre équation analogue à celle qui donne l'addition des «intégrales elliptiques». Ces intégrales ne s'expriment pas par des fonctions élémentaires (les quatre opérations, l'exponentielle, le logarithme et les fonctions sinus et cosinus) ; elles sont égales aux aires comprises entre l'axe des abscisses et les courbes de la forme $y = R(x, \sqrt{P(x)})$, où R est une fonction rationnelle et où P est un polynôme à une variable de degré trois ou quatre).

Euler a donné une démonstration du théorème de Fermat pour l'exposant égal à 3 ; il y fait une première allusion dans une lettre à Goldbach, en août 1753, puis, en 1759, dans un article consacré aux formes quadratiques $a^2 + 3b^2$ et $m^2 + mn + n^2$: on passe de l'une à l'autre en posant $m = a + b$ et $n = b - a$, et Euler annonce que si t^3 est représenté par la seconde forme, il en est de même de t , ce qui lui permet d'amorcer une démonstration par descente infinie. Il publie une démonstration dans son *Algèbre*, en 1770, où il utilise des nombres complexes de la forme $a + b\sqrt{-3}$ (où a et b sont des nombres entiers), en admettant que ces nombres ont une décomposition en facteurs premiers comme les entiers ordinaires : tout nombre de cette forme se décompose en un produit unique de nombres «premiers» du même type.

Cependant il remarque que l'équation $x^3 + y^3 + z^3 = t^3$ est possible : c'est le problème 16 du livre V de Diophante, qu'il étudie dans un article de 1756. Il

pense qu'une somme de trois bicarrés ne peut être un bicarré, tandis qu'une somme de quatre bicarrés peut être un bicarré (l'équation correspondante, $x^4 + y^4 + z^4 + t^4 = u^4$, ne sera résolue qu'en 1911 par le mathématicien américain M. Norrie). Euler croyait encore qu'une somme de quatre puissances cinquièmes ne peut pas être une puissance cinquième, mais, en 1962, M. Birch a trouvé un contre-exemple par ordinateur, démontrant ainsi que cette idée était fausse.

Joseph Louis Lagrange (1736-1813) a pris le relais d'Euler pendant la dizaine d'années où il s'est intéressé à la théorie des nombres. Lagrange obtient d'abord un résultat sur la périodicité des fractions continues de nombres quadratiques : les nombres quadratiques sont les racines d'équations du deuxième degré dont les coefficients sont des nombres entiers (par exemple, $\sqrt{3}$ est un nombre quadratique, parce qu'il est solution de l'équation $x^2 - 3 = 0$). On peut écrire ces nombres sous la forme de fractions continues, de la forme générale $1 + 1/(a_0 + 1/(a_1 + 1/(a_2 + 1/(...))))$; notamment $\sqrt{3}$ s'écrit sous la forme $1 + 1/(1 + 1/(2 + 1/(1 + 1/(2...))))$ dont la périodicité est égale à deux : les 1 et les 2 alternent aux dénominateurs successifs.

À partir de ce résultat, Lagrange établit la possibilité de l'équation de Pell-Fermat dans le cas général. Puis il obtient un critère d'existence d'une solution pour les équations diophantiennes de degré deux (critère qui sera amélioré par Adrien Marie Legendre). Lagrange n'aborde les équations de degré trois ou quatre que dans un article de 1777, où il utilise, sous une forme exclusivement algébrique, la méthode de la tangente.

L'analyse diophantienne au XIX^e siècle

Au XIX^e siècle, de nouveaux cas de la conjecture de Fermat sont progressivement établis : Peter Dirichlet (1805-1859), alors étudiant à Paris, démontre en 1825 l'impossibilité de l'équation $x^5 \pm y^5 = 2^m z^5$, avec m positif, par une descente infinie fondée sur les propriétés des nombres de la forme $a + b\sqrt{5}$. La même année, Legendre démontre le théorème de Fermat pour l'exposant 5. Puis, en 1832, Dirichlet établit le cas de l'exposant 14 au moyen de l'arithmétique des nombres de la

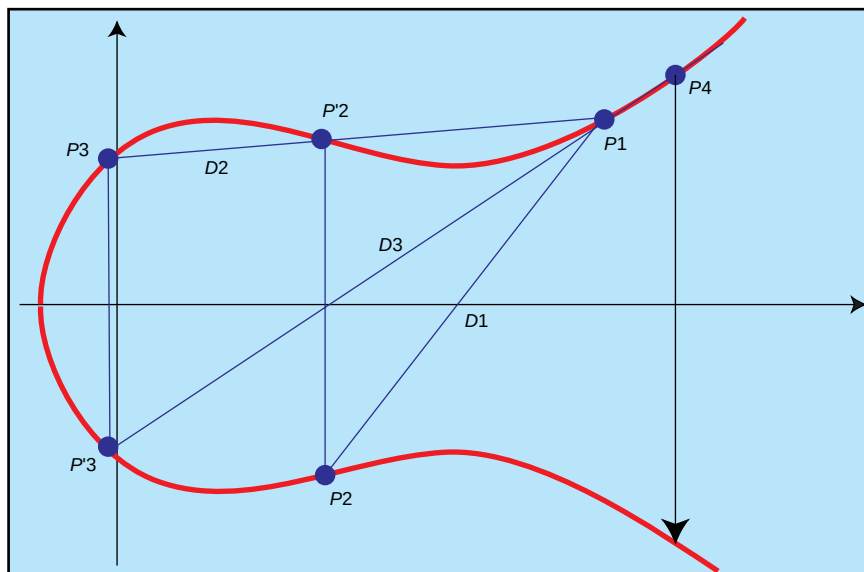
forme $m + n\sqrt{-7}$, où m et n sont nombres entiers, et Gabriel Lamé (1795-1870), en 1839, obtient une démonstration pour l'exposant 7.

Dans les mêmes années, Legendre, Niels Abel (1802-1829) et Sophie Germain (1776-1831) mettent au point des méthodes élémentaires pour atteindre des résultats sur l'impossibilité du premier cas de l'équation de Fermat $x^p + y^p + z^p = 0$, avec p premier impair ne divisant aucun des nombre x, y, z . Sophie Germain démontre que ce cas est impossible s'il existe un nombre premier q tel que p ne soit pas une puissance p -ième modulo q : lorsque $2p + 1$ est premier, par exemple si $p = 11$ ($2p + 1 = 23$), on peut prendre $q = 2p + 1$ parce que 11 n'est pas une puissance onzième modulo 23 (tout nombre compris entre 1 et 22, élevé à la puissance 11, est un multiple de 23 augmenté ou diminué de 1). Et Legendre étend ce résultat au cas où $4p + 1$ est premier, par exemple si $p = 13$ ($4p + 1 = 53$).

Le premier travail d'Ernst Kummer (1810-1893), en 1837, sur l'équation de Fermat se rattache au même ordre d'idées ; il établit d'abord que si l'équation $x^{2\lambda} + y^{2\lambda} = z^{2\lambda}$ a une solution telle que λ n'ait pas de facteur commun avec le produit xyz , alors λ a un reste égal à 1 dans la division par 8.

Apparemment Kummer a initialement cru qu'il pourrait démontrer le théorème de Fermat pour un exposant λ premier impair quelconque par une méthode de descente infinie, au moyen de l'arithmétique des nombres cyclotomiques engendrés par α , une racine λ -ième de 1, envisagée par Gauss dans la septième section de ses *Disquisitiones arithmeticae* : les nombres cyclotomiques sont les nombres de la forme $a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{\lambda-2}\alpha^{\lambda-2}$, où les nombres $a_0, a_1, a_2, \dots, a_{\lambda-2}$ sont des nombres entiers, et où α est une racine λ -ième de l'unité, c'est-à-dire un nombre complexe vérifiant l'équation $x^\lambda = 1$; un tel nombre est représentable par un point du cercle de rayon centré sur l'origine (on peut considérer que l'arc de cercle qui se trouve entre 1 et α est la λ -ième partie de tout le cercle). Si les entiers cyclotomiques avaient admis une décomposition unique en facteurs premiers, une solution (x, y, z) de l'équation de Fermat pour l'exposant λ , sans facteur commun avec x, y et z , aurait conduit à l'égalité :

$$z^\lambda = (x + y)(x + \alpha y) \dots (x + \alpha^{\lambda-1}y)$$



7. SUITE DE POINTS créée à partir d'une solution **P1** de l'équation associée à la courbe en rouge. **P1** serait une solution dite « de torsion » si l'une des droites **D** était verticale. Les points de torsion forment des groupes dont on a exploré les relations avec les points rationnels.

avec, au second membre, λ nombres sans facteurs communs ; on aurait déduit que ces facteurs devaient être tous des puissances λ -ièmes, ce qui aurait permis d'amorcer une descente infinie.

Toutefois Kummer découvrit en 1844 que l'arithmétique des entiers cyclotomiques était délicate : il n'existe pas toujours de décomposition unique de ces nombres en facteurs cyclotomiques premiers. Pour se raccrocher à l'arithmétique des entiers naturels, Kummer considère la norme des entiers cyclotomiques $f(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{\lambda-2}\alpha^{\lambda-2}$: cette norme, définie par le produit $f(\alpha)f(\alpha^2) \dots f(\alpha^{\lambda-1})$, est toujours un nombre entier naturel, et la norme d'un entier cyclotomique premier est un nombre premier ordinaire, de reste égal à 1 dans la division entière par λ .

Réciproquement, pour les nombres premiers inférieurs à 1 000, Kummer a laborieusement calculé (à la main, parce qu'il ne disposait alors pas d'ordinateur) des tables de factorisation en entiers cyclotomiques premiers des nombres premiers ordinaires ayant pour reste 1 dans la division entière par λ , pour tous les nombres λ inférieurs à 24. Il a ainsi découvert que, pour λ égal à 23, le nombre premier ordinaire 47 (deux fois 23 plus 1) n'est pas la norme d'un entier cyclotomique, de sorte que les entiers cyclotomiques engendrés par une racine 23-ième de l'unité n'admettent pas de décomposition unique

en facteurs premiers. Cela a conduit Kummer à élaborer, dans ses travaux suivants, sa théorie des « nombres premiers idéaux », qu'il ne définissait d'ailleurs pas comme des nombres : il donnait seulement les conditions pour qu'un entier cyclotomique soit divisible par une puissance donnée d'un tel nombre idéal. En termes modernes, les nombres idéaux de Kummer peuvent s'interpréter comme des fonctions associant un nombre entier naturel à chaque entier cyclotomique, avec des conditions particulières ; l'exposant de la puissance du nombre idéal qui divise l'entier cyclotomique est précisément cette fonction.

Kummer définit les produits d'idéaux (on les appelleraient aujourd'hui des diviseurs), qu'il groupe en un nombre fini h de classes. En reprenant des idées de Dirichlet, il étudie ce nombre de classes au moyen d'une fonction analogue à la fonction zêta de Riemann (le produit, sur tous les idéaux p premiers, de termes de la forme $1 / (1 - n(p)^{-s})$, où $n(p)$ représente la norme de p). La finitude du nombre de classes permet d'écrire les facteurs $x + \alpha^k y$ de z^λ comme des puissances λ -ièmes multipliées par des facteurs ne pouvant prendre qu'un nombre fini de valeurs. Lorsque λ ne divise pas le nombre de classes, on peut poursuivre la démonstration comme dans le cas où h est égal à 1 (celui de l'arithmétique ordinaire) ; on dit alors que λ est un nombre premier régulier, et Kummer a donné un critère pour reconnaître les nombres

premiers réguliers. Les seuls nombres premiers irréguliers inférieurs à 100 sont 37, 59 et 67.

Analyse diophantienne et géométrie algébrique

Le travail de Newton précédemment évoqué à propos de tangentes et de sécantes (inconnu jusque dans les années 1960) était resté sans suite, mais la connexion de l'analyse diophantienne avec le calcul intégral fut explicitée pour le cas des intégrales elliptiques par Carl Jacobi (1804-1851) dans une courte note publiée en 1834. Jacobi y interprète la méthode d'Euler pour construire des solutions rationnelles de l'équation $y^2 = P(x)$, où P est un polynôme de degré égal à 4, au moyen de la multiplication par un entier de l'intégrale de la fonction $1/\sqrt{P(x)}$.

James Sylvester (1804-1897), à l'Université de Londres, a consacré des travaux remarquables à l'étude des équations diophantiennes de degré égal à 3 par la géométrie algébrique. Il annonce ses résultats dans une note de 1858 et il les développe dans une série de mémoires en 1879 et en 1880. Sa méthode consiste à construire des points rationnels d'une courbe cubique (voir la figure 5) à partir d'un point rationnel donné en se servant de tangentes et de sécantes.

En 1890, le dernier mathématicien capable d'embrasser l'ensemble des mathématiques, David Hilbert (1862-1943), et son professeur Adolf Hurwitz (1859-1919) étudient systématiquement les équations diophantiennes à l'aide de la notion de genre d'une courbe, introduite par Rudolf Clebsch (1833-1872), à la suite de travaux de Bernhard Riemann : on étend la méthode de la corde en remplaçant la sécante (de degré 1) qui coupe la cubique (de degré 3, soit $1 + 2$) par une courbe de degré inférieur de deux unités au degré n de la courbe étudiée et en imposant que cette courbe passe par tous les points singuliers (points doubles, points de rebroussement, etc). On lui impose en outre de passer par un certain nombre de points ordinaires. Si p est le genre, ce nombre de points imposés doit être égal à $n - 2 + p$, et il reste p points d'intersection. Hilbert et Hurwitz se limitent au genre égal à zéro ; ils trouvent que l'on peut passer, par des quotients de polynômes à coefficient rationnels (des «transformations birationnelles»), de courbes de genre

égal à zéro et de degré n définies sur l'ensemble des nombres rationnels à une droite ou à une conique, et inversement. En réduisant ainsi le degré d'une équation diophantienne, ils arrivent au degré 1 ou 2, que l'on sait résoudre.

Puis, en 1901, Henri Poincaré (1854-1912), sans connaître apparemment le travail de Hilbert et de Hurwitz, consacre un article important à l'analyse diophantienne. Poincaré voulait classer les problèmes diophantiens en problèmes équivalents par certaines transformations adaptées à la nature du problème. Comme il s'intéressait à l'analyse diophantienne rationnelle, les transformations birationnelles à coefficients rationnels se présentèrent naturellement, et le genre, qui n'est pas modifié au cours de telles transformations (on dit que c'est un invariant birationnel) a une signification que n'a pas le degré. Poincaré traite d'abord le cas du genre zéro, obtenant le même résultat que Hilbert et Hurwitz ; puis il passe au genre un, qui occupe l'essentiel de son mémoire.

Poincaré montre que les courbes de genre un qui ont un point rationnel sont birationnellement équivalentes à la cubique déjà considérée, d'équation $y^2 = 4x^3 - ax - b$. Il introduit les fonctions dites elliptiques afin d'exprimer les coordonnées des points de ces courbes.

Un ensemble de points rationnels d'une cubique plane est dit stable par la construction des tangentes et des sécantes si cette construction ne fait pas sortir de l'ensemble. Dans une suite d'articles publiés entre 1906 et 1908, Beppo Levi cherche ces systèmes stables. En termes modernes, il s'agit de déterminer quels sont les groupes de torsion possibles dans le groupe des points rationnels (voir la figure 7). La détermination complète a été faite par Bruno Mazur, en 1978, et il est remarquable que Levi s'en soit approchée.

Contrairement à Poincaré, L. Mordell s'intéressait à l'analyse diophantienne entière ; en 1922, il voulait établir la finitude du nombre de solutions entières d'équations diophantiennes de la forme $y^2 = P(x)$, où P est un polynôme de degré trois ou quatre. Pour le degré trois, la théorie des nombres algébriques lui permettait de se ramener à un théorème d'Axel Thue, lié à la théorie des approximations diophantiennes (comment estimer la rapidité de l'approximation d'un nombre irrationnel par une

suite de nombres rationnels), sur la finitude du nombre de solutions entières d'une équation de la forme $F(u,v) = m$, où F est un polynôme homogène en (u,v) , c'est-à-dire dont le degré total, pour u et pour v soit égal pour tous les termes du polynôme (par exemple, le polynôme $uv^3 + u^2v^2 + 4v^4$ est homogène, et de degré égal à quatre) ; mais cette méthode était inopérante en degré quatre.

Mordell s'est aperçu qu'elle lui donnait un procédé de descente conduisant à établir que les points rationnels s'obtiennent à partir d'un nombre fini d'entre eux par la construction des tangentes et des sécantes ; c'est alors seulement qu'il cite Poincaré et qu'il formule sa célèbre conjecture, sur la finitude du nombre de points rationnels pour les genres strictement supérieurs à un.

André Weil, en 1929, a réinterprété le résultat de Mordell en termes du groupe des points rationnels d'une courbe elliptique. La conjecture de Mordell a fini par être démontrée en 1983, par l'Allemand Gerd Faltings, qui a suivi une autre voie. Comme la courbe de Fermat est de genre supérieur à un lorsque l'exposant est strictement supérieur à trois, le théorème de G. Faltings indique que l'équation de Fermat n'a au plus qu'un nombre fini de solutions.

Le théorème de Fermat proprement dit est sorti de son isolement plus récemment, en 1987, quand on s'est aperçu qu'il se déduisait de conjectures formulées de manière complètement indépendantes. Notamment un théorème de Kenneth Ribet a montré que le théorème de Fermat est une conséquence d'une conjecture de M. Taniyama et de A. Weil sur les courbes elliptiques ; c'est cette conjecture que A. Wiles vient de démontrer.

Christian HOUZEL est professeur de mathématiques à l'IUFM de Paris.

O. NEUGEBAUER et A. SACHS, *Mathematical Cuneiform Texts*, New Haven, 1945.

DIOPHANTE, *Les Arithmétiques*, 4 vol., Éditions Allard et Rashed, Paris, vol. 3 et 4, 1984 ; vol. 1 et 2 à paraître.

G. TERJANIAN, *Fermat et l'analyse diophantienne*, *Sém. d'Hist. des Math. de Toulouse* 8, pp. 57-66, 1986.

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