

Chapitre 5

L'académie des quarante problèmes

Le plaisir de découvrir — ou redécouvrir — les mathématiques dans un livre de réflexion passe, de manière pratiquement obligatoire, par l'histoire de ses grandes périodes créatrices. Plutôt que d'évoquer, comme dans un manuel destiné à des étudiants, les tournants les plus féconds au fur et à mesure du déroulement des siècles, nous adoptons ici une forme plus proche d'un dictionnaire raisonné, en regroupant arbitrairement quarante « problèmes », ou plutôt quarante questionnements, associés à des noms propres, essayant de couvrir tant bien que mal toutes les branches qui ont compté dans le développement des mathématiques : logique, statistique aussi bien que théorie des équations algébriques...

Comme tout choix, le nôtre est largement critiquable. Cela reconnu bien volontiers, nous espérons que, par l'intermédiaire de cette Académie mathématique virtuelle — on aurait pu également parler de caverne aux quarante créateurs, ou des quarante chercheurs qui ont fait les mathématiques —, quelque chose de la curiosité indomptable de ces fondateurs d'empire pourra toucher des lecteurs, qui auront envie d'en savoir plus.

Une telle énumération, et les autres chapitres de ce volume, doivent naturellement beaucoup aux livres d'histoire des mathématiques existants. Nous avons particulièrement consulté avec profit *A History of Mathematics* de Carl B. Boyer (Princeton University Press, édition de 1985), *Mathematical Thought from Ancient to Modern Times* de Morris Kline (Oxford University Press, édition de 1976), *History of Mathematics* de D.E. Smith (Dover Publications, édition de 1958 en deux volumes), *Abrégé d'histoire des mathématiques* de Jean Dieudonné *et al.* (Hermann, édition de 1986), ainsi que *Pour l'honneur de l'esprit humain* de Jean Dieudonné (Hachette, édition de 1987), *Histoire des mathématiques* de Jean Itard (Larousse, édition de 1977, épuisé), *Histoire des mathématiques* de Jean-Paul Collette (diffusion Vuibert, édition de 1973 en deux volumes), *Histoire abrégée des sciences mathématiques* de Maurice d'Ocagne et René Dugas (Vuibert, édition de 1955, épuisé), mais aussi les grands classiques, moins

ambitieux, d'Eric Temple Bell (*Les Grands Mathématiciens* chez Payot, épuisé), de Pierre Dedron et Jean Itard (*Mathématiques et Mathématiciens* chez Magnard, également épuisé), la compilation des *Notes historiques* de Nicolas Bourbaki chez Masson, et naturellement des ouvrages spécialisés comme ceux de L.E. Dickson sur la théorie des nombres, où l'ouvrage collectif *Les Nombres* tout récemment traduit de l'allemand chez Vuibert.

Citer toutes nos autres sources serait presque impossible, et certainement lassant. Cela dit, c'est avec grand plaisir que nous reconnaissons avoir également puisé beaucoup de renseignements, notamment des dates, titres de livres, anecdotes, etc., dans le récent et très riche dictionnaire *Des mathématiciens de A à Z* de Bertrand Hauchecorne et Daniel Suratteau (Ellipses, édition de 1996), ainsi que sur certains sites Internet bien connus.

Enfin nous devons rappeler que le recours direct aux œuvres originales de certains des grands créateurs célébrés ici est encore la meilleure façon d'essayer de comprendre l'histoire des idées, même compte tenu des difficultés très réelles qu'il y a à interpréter correctement des textes écrits à une époque parfois très éloignée de la nôtre. En dehors de la consultation des œuvres complètes, nous avons utilisé des recueils d'extraits (*Mathématiques au fil des âges* chez Gauthier-Villars en français (1987), mais aussi les « *source books* » anglo-saxons, comme ceux de D.E. Smith, D.J. Struik ou celui de l'Open University), ainsi que la compilation *The World of Mathematics* de J.R. Newmann (4 volumes chez George Allen & Unwin, 1956).

Le problème d'Apollonius (262-190)

Tracer à la règle non graduée et au compas un cercle tangent à trois cercles donnés.

Ce problème a traversé l'histoire : si nous ignorons la solution d'Apollonius lui-même, nous savons que Descartes, Fermat et Newton, puis Cauchy et surtout Joseph Gergonne (1771-1859) lui ont apporté chacun une solution plus ou moins astucieuse, toutes si diverses qu'on peut difficilement les résumer (une remarque simplement : on peut se ramener facilement au cas où l'un des cercles a été réduit à un point, en augmentant ou diminuant le rayon du cercle cherché). Le problème admet a priori huit solutions, à savoir un cercle qui est tangent extérieurement aux trois cercles C_1 , C_2 , C_3 considérés, un cercle qui leur est tangent intérieurement, et deux fois trois cercles tangents extérieurement et intérieurement. On notera que si C_1 , C_2 , C_3 sont les cercles ex-inscrits d'un triangle, une solution est donnée par son cercle d'Euler (théorème de Feuerbach).

Nous citons ici cette question, que la qualité des intervenants montre ne pas être tout à fait sans intérêt, essentiellement pour saluer l'innombrable cohorte des problèmes de géométrie plane ou de l'espace qui a toujours fasciné, outre des professionnels, des foules d'amateurs passionnés. Aujourd'hui encore ces cercles d'Apollonius ne sont pas complètement morts, puisqu'on en retrouve une trace dans l'un des problèmes du Concours général français de l'année mondiale des mathématiques !

La baderne d'Apollonius

Le problème de la baderne d'Apollonius consiste à remplir de cercles l'espace compris entre trois cercles C_1, C_2, C_3 , dont, pour simplifier, on admettra que le rayon est le même. L'opération commence par le tracé du cercle γ tangent à C_1, C_2, C_3 , dont le centre est celui du triangle $O_1 O_2 O_3$. Ce seront ensuite le cercle γ_1 tangent à C_1, C_2 et γ , le cercle γ'_1 tangent à C_1, C_2 et γ_1 , le cercle γ'' tangent à γ, γ_1 et C_1 , et ainsi de suite de façon fractale dans toutes les parties du triangle curviligne ABC .

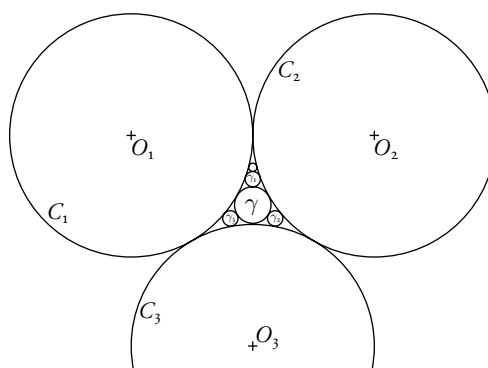


figure 32. La baderne d'Apollonius

Ces cercles laissent une aire lacunaire L , de plus en plus petite au fur et à mesure que leur nombre augmente. La question est encore entière de savoir si L tend vers zéro ou vers une valeur limite différente de zéro.

NB : Le nom d'Apollonius hante les mathématiques. Ainsi, étant donné un triangle ABC dont les bissectrices issues de A coupent en B' et C' le côté BC , le cercle de diamètre $B'C'$ (qui passe par A) est l'un des trois cercles dits d'Apollonius du triangle ABC . Les deux autres s'obtiennent en opérant de la même manière pour B et pour C . Ces trois cercles d'Apollonius, dont les centres se trouvent sur une droite dite de Lemoine, ont le même axe radical (axe de Brocard).

Le problème d'Archimède (287-212)

Qu'est-ce qu'une longueur ? une aire ? un volume ?

Voici le très lointain début de l'analyse en général et du calcul intégral en particulier. L'un de nos quasi-contemporains, Henri Lebesgue, trouvera encore de quoi renouveler profondément ce terrain où Archimède a été un précurseur plus de vingt et un siècles plus tôt.

Ses travaux sur la longueur du cercle le conduiront, comme on l'a vu plus haut, à donner une première valeur de π basée sur une démonstration forte. Il déterminera, parfois grâce à l'aide de sommations de séries géométriques, des aires de parties du plan délimitées par des coniques (ellipses et segments de paraboles) ou par d'autres courbes qu'il invente, comme la spirale qui porte son nom. Il calculera également des volumes et des centres de gravité, qui seront admirés et imités par un Fermat au XVII^e siècle.

Cela dit, le fait qu'il ait fallu attendre près de deux mille ans pour créer ces deux calculs, pour lesquels Archimède avait déjà franchi les premiers pas, est en soi une énigme irritante.

Le problème de Bourbaki (né en 1935)

Écrire un traité basique universel des mathématiques.

Bien sûr, Nicolas Bourbaki — sur lequel commencent à paraître de bons livres — n'a pas existé en tant que mathématicien puisque tout théorème nouveau démontré par l'un des auteurs de ce *Traité* était publié par ailleurs sous le nom propre de son découvreur. Mais il a presque réussi à remplir son projet utopique, sous l'égide de Hilbert et Sophus Lie (1842-1899), et laissera un sillage prestigieux.

Il est cité ici parce qu'il fut à l'origine d'une tentative « pédagogique » remarquable, à l'usage des seuls mathématiciens, non des pédagogues, dans la ligne du formalisme à la Hilbert. La réputation internationale de ce travail formidable, initié par quelques jeunes normaliens nés entre 1900 et 1920, fut exemplaire (toutes proportions gardées, Bourbaki fut l'Euclide du XX^e siècle). Cette influence a eu des effets très positifs quant à une normalisation du vocabulaire et des notations, par exemple en topologie ou en analyse fonctionnelle, tandis que des idées fortes comme celle d'algébrisation et de linéarisation de l'analyse se voyaient par là admises par tous. De plus, un séminaire très fameux portant son sigle réunit toujours à Paris les principaux mathématiciens français, avides des avancées les plus importantes de la discipline.

Cela dit, de nombreux pans des mathématiques n'ont jamais été traités par les bourbakistes, particulièrement dans les applications, mais aussi dans la théorie des

nombres, ou des catégories. On peut le regretter, mais Bourbaki ne verra sans doute plus jamais spontanément venir à lui les meilleurs de chaque promotion, de son école nourricière. S'il est mort, séminaire trimestriel excepté, il a fortement marqué son temps, et l'on ne fera plus tout à fait des mathématiques dans l'avenir comme on les aurait faites s'il n'avait pas lancé son orgueilleux défi unitaire.

Le problème de Burnside (1852-1927)

Classifier les groupes finis simples.

Notre énoncé n'est pas tout à fait correct car William Burnside n'a pas explicitement fixé ce but à ses successeurs. Cela dit, la publication de son livre de 1911 et la mise au point d'un certain nombre de conjectures importantes qui y figurent ont montré par la suite qu'un tel travail était envisageable.

Walter Feit et John Thompson ne démontreront qu'en 1963 la plus importante d'entre elles (tout groupe fini de cardinal impair est résoluble) à l'aide d'une méthode par l'absurde pour laquelle, aujourd'hui encore, on a besoin de plus d'une centaine de pages ! Il en avait fallu deux cent cinquante-quatre dans le mémoire original.

Les années quatre-vingt ont vu aboutir un travail de toute une communauté pour recenser, en 1 500 pages cette fois, la totalité des groupes finis simples. Il existe ici un parallèle curieux avec les mises en commun de plus en plus fréquentes de centaines d'ordinateurs personnels pour « casser » un nombre en facteurs premiers. Qui a prétendu que les mathématiciens ne savaient pas travailler en équipe ?

L'un de ces groupes est si complexe, gros et spécial (sporadique, dans le langage de ces chercheurs), qu'il a reçu le doux surnom de *Monstre*. Le plaisir des mathématiciens est parfois légèrement décalé, mais pas leur humour. Le cardinal de ce groupe est supérieur à 10^{53} ; on sait depuis 1983 qu'il n'existe que vingt-cinq autres groupes simples finis ne se rattachant à aucune théorie générale.

Le problème de Cantor (1845-1918)

Y a-t-il quelque chose entre le dénombrable et le continu ?

Le créateur de la théorie des ensembles est Georg Cantor, analyste classique mais de grand talent, spécialiste des séries de Fourier qui fut conduit à découvrir des structures fort abstraites pour démontrer un théorème très intuitif d'unicité de coefficients.

Pour ce faire, il a développé des techniques très nouvelles, comme en 1873 le procédé diagonal souvent mis à toutes les sauces après lui (voir Gödel, 1931, par exemple). Il a légué à la génération suivante le célèbre problème du continu : est-il vrai que toute partie du corps des réels \mathbb{R} puisse être mise en bijection, soit avec l'ensemble \mathbb{N} des entiers naturels, soit avec \mathbb{R} lui-même ? Ou encore : y a-t-il un ensemble dont le cardinal soit strictement compris entre celui de \mathbb{N} et celui des parties de \mathbb{N} ?

Ce qui est intéressant ici, c'est que la réponse est venue en deux temps. En 1938, Kurt Gödel démontre qu'on ne pourra jamais prouver que cette conjecture est fautive dans le cadre de l'axiomatique des ensembles dite de Zermelo-Fraenkel ; en 1963 Paul Cohen (né en 1934) démontre qu'on ne pourra jamais prouver le contraire, apportant ainsi un exemple frappant de proposition indécidable. (Il en va d'ailleurs de même pour l'axiome du choix de Zermelo.)

Le nom de Cantor a souvent été, surtout en France, lié à de vives polémiques concernant les mathématiques dites « modernes ». Les arguments les plus bas ont été utilisés, par exemple le fait que ce précurseur, en conflit avec ses confrères, finit ses jours dans un asile d'aliénés. Mais que l'on se rassure : sa notoriété et la fécondité de ses idées sont largement assurées pour les siècles à venir.

Le problème de Cavalieri (1598-1647)

Qu'est-ce qu'un infiniment petit ?

Nous avons choisi de parler ici de Bonaventure Cavalieri plutôt que d'autres précurseurs du calcul infinitésimal pour diverses raisons, dont le fait qu'il a été le premier à oser parler explicitement d'*indivisibles*. Il est difficile de dire s'il a effectivement démontré tout ce qu'il affirme dans un livre capital en 1635 — par exemple les valeurs de certaines aires et volumes, équivalentes à l'intégration des monômes x^n où n est naturellement entier positif —, car ses prémisses, vers 1626, sont beaucoup trop confuses.

L'idée fondamentale est que l'on peut découper un solide (disons : un cône ou une pyramide) en un nombre indéfini de tranches très fines et le recomposer sous une autre forme sans modifier sa mesure. C'est cela qui lui permet d'obtenir des résultats très proches de ce que donnera le calcul intégral moins de quarante ans plus tard (voir notre description des disques d'Archimède).

Toutefois, la distance de Cavalieri à un Leibniz reste immense ; ses puissants indivisibles ne sont guère assimilables aux infiniment petits qui seront à la base de la révolution qu'il n'a pas bien su voir venir. Que ses mânes nous permettent de citer l'une de ses affirmations les plus contestables : *la rigueur est l'affaire de la philosophie*,

pas celle de la géométrie. Aurait-il été partisan de l'idée selon laquelle le travail des mathématiciens est de fournir des recettes toutes prêtes ? Nous aurions alors bien du mal à le lui pardonner.

Le problème de César (101-44)

Un message peut-il rester privé ?

Le nom de ce général et homme d'État romain peut surprendre dans un livre mathématique. Jules César mérite pourtant d'être au moins évoqué pour deux raisons : son calendrier julien, qu'affinera Grégoire XIII, et son utilisation pendant la guerre des Gaules d'un système de cryptographie, régulièrement réinventé par des écoliers turbulents (question : découvrir quel lycéen se cachait, dans les années cinquante, sous le pseudonyme d'Epfsi Xesatgim, qui avait compliqué le jeu en distinguant consonnes et voyelles).

De grands mathématiciens, dont Viète et Alan Turing (1912-1954), ont consacré une partie non négligeable de leur recherche à ce domaine, dans les deux cas pour des raisons politiques. Le premier était un haut fonctionnaire au service d'Henri IV, qui désirait lire les dépêches cryptées des armées de Philippe II, et le second contribua à la création de proto-ordinateurs destinés à casser pour le compte de Winston Churchill les messages de la Kriegsmarine écrits grâce à la machine *Enigma*.

Chacun sait que cette cryptographie ancienne, même devenue aussi subtile, a été bouleversée en 1976 par l'invention, d'abord théorique puis vite suivie d'effets pratiques, des *systèmes à clefs publiques*. Voir sur ce sujet, qui mériterait de bien plus amples développements, notre chapitre sur l'informatique mathématique et le passionnant *Histoire des codes secrets* de Simon Singh (J.-C. Lattès, 2000).

Nous n'ajouterons qu'un bref commentaire : dans une science, il est impossible de prévoir les parties qui vont exploser et connaître un renouvellement complet. Mais dans ce cas précis il est extraordinaire que l'essentiel de la révolution soit basée sur des astuces parfois si élémentaires qu'un contemporain intelligent d'Euler aurait parfaitement pu les trouver. Pour une fois, une envolée fondamentale n'est pas due à une accumulation de progrès techniques, mais simplement à des idées totalement sans précédent. Il faut ajouter aussi que l'évolution de la société (problèmes d'espionnage, mais aussi développement effréné des communications bancaires) a rendu si nécessaires de nouvelles méthodes qu'elles ont fini par arriver, pour notre plus grand plaisir.

Le problème de d'Alembert (1717-1783)

Tout polynôme complexe non constant a au moins une racine complexe.

C'est à la suite d'une erreur, validée par la tradition, que le théorème cité ici porte le nom de d'Alembert, qui n'a été ni le premier à l'énoncer — Albert Girard (1595-1632) puis René Descartes le précédèrent — ni à le démontrer correctement : il faudra attendre la thèse de Gauss en 1799, qui y reviendra à de nombreuses reprises.

Toutefois d'Alembert mérite d'être cité car sa propre tentative de 1746 n'était pas très éloignée de ce qui était possible à son époque. Rappelons que d'Alembert joua un grand rôle dans la diffusion des idées du calcul différentiel et intégral, notamment par ses articles de l'*Encyclopédie*, et qu'il a donné son nom à un prix prestigieux de la Société mathématique de France.

Le problème de De Beaune (1601-1652)

La première inversion du problème des tangentes.

L'histoire des logarithmes, qui ont précédé de bien loin la notion de fonction logarithme, est une fresque aux racines anciennes puisque commencée avec Neper et Jobst Bürgi (1552-1632) ; elle ne se termine qu'avec Euler et enfin Cauchy. Florimond de Beaune est surtout connu comme disciple de l'algébriste Descartes, le premier à avoir en quelque sorte étudié une équation différentielle dont la fonction logarithme est justement solution.

À l'époque, où le nom et a fortiori le concept même de dérivée sont impossibles à imaginer, il en va forcément de même pour ceux de primitive. Toutefois, calculer une dérivée au début du XVII^e siècle revient à savoir tracer une tangente à une courbe : on peut comprendre comment le problème de De Beaune, connu sous ce nom dans l'histoire, pouvait se glisser par une mince faille dans l'orgueilleux système cartésien qui ne voulait connaître que les courbes algébriques. On peut voir là une très timide ébauche de calcul intégral.

Le problème de Dedekind (1831-1916)

Qu'est-ce qu'un nombre ?

Les noms de Richard Dedekind et de Giuseppe Peano (1858-1932), qui ont donné respectivement en 1888 et 1889 des axiomes pour \mathbb{N} , s'imposent si l'on parcourt l'immense zoo des nombres (voir le chapitre qui leur est consacré). Le second a

reconnu l'influence du premier sur sa recherche, mais les objectifs des deux systèmes sont très différents.

Dedekind fut aussi l'un des pères de l'axiomatique de \mathbb{R} , ainsi qu'un grand algébriste, créateur de la théorie des idéaux des anneaux, ami et disciple de Cantor qu'il aida à construire la théorie des ensembles. Outre son travail axiomatique et l'invention d'un symbolisme pratiquement encore utilisé de nos jours, Peano fut l'un des premiers à préciser en 1887 ce que pourrait être une notion de mesure pour les parties du plan. Camille Jordan (1838-1922) en 1893, puis Émile Borel en 1898, Henri Lebesgue en 1901 et enfin Andreï Kolmogorov (1903-1987) en 1933 (*Grundbegriffe der Wahrscheinlichkeitsrechnung*) en tireront parti pour créer l'intégration et le calcul des probabilités modernes.

Le problème de Descartes (1596-1650)

La réfraction et les Ouales.

Dans l'œuvre immense de Descartes, certaines parties, exposées brièvement dans son unique ouvrage de mathématicien *La Géométrie*, prouvent sa puissante originalité comme scientifique et posent, par là-même, des questions difficiles à l'historien.

Il s'agit par exemple d'une solution au problème général des tangentes, ou plutôt des normales, la première à avoir été publiée tandis que Fermat et Roberval (peut-être Torricelli) en avaient élaboré d'autres, respectivement basées sur une sorte de version grossière de dérivée (voir le chapitre sur le calcul différentiel et intégral) et de compositions de mouvements.

Descartes définit au contraire une normale comme la droite passant par le centre d'un cercle coupant la courbe de façon à obtenir une équation admettant une racine multiple au point considéré. C'est assez étrange et plutôt malcommode, mais l'idée est révolutionnaire. Elle sera toujours utilisée, sous une forme légèrement différente, en géométrie algébrique sur des corps où la notion de racine double a toujours un sens tandis que celle de limite n'en a pas faute de topologie.

Si l'on peut imaginer d'où vient cette théorie (sans doute une retombée de sa méthode générale de résolution d'une équation algébrique en coupant certaines courbes par des cercles, où le cas particulier de racines doubles n'avait pu lui échapper), on est par contre complètement ignorant de ce qui l'a conduit aux célèbres Ouales de Descartes, réglant un problème d'optique majeur, l'astigmatisme d'une surface par rapport à deux points, au prix de ce qui paraît toujours comme le résultat d'une sorte de divination.

Aujourd'hui, ce problème est enlevé en quelques minutes par une simple équation différentielle. C'était hors de question à l'époque de *La Géométrie*, même si ce ne sera pas le seul contact de Descartes avec cette notion (voir de Beaune). Donc le mystère est entier. On peut seulement constater, frustré, que les courbes très nouvelles qu'il définit, à l'aide d'un système de coordonnées très spécial venu de la géométrie des coniques, répondent bien à sa question. C'est un *deus ex machina*, venu de nulle part, forçant au respect, mais totalement opaque dans sa présentation.

Oubliant Descartes et même Fermat, oubliant *a fortiori* les remarquables travaux grecs sur les coniques ou quelques courbes particulières comme la spirale d'Archimède, il reviendra à Newton puis à Leibniz de régler apparemment le problème des tangentes pour l'éternité. Cela dit, même aujourd'hui, on peut être conduit à définir des tangentes à des courbes qui demandent des études infinitésimales beaucoup plus subtiles qu'avec les boîtes noires patiemment mises au point par les maîtres d'école statufiant le calcul différentiel en une suite de recettes. Le problème des tangentes n'est pas encore devenu sans intérêt, même au siècle des calculettes !

Le problème d'Ératosthène (276-194)

Comment déterminer les nombres premiers, et factoriser tout entier en produit de diviseurs premiers ?

RSA : ces trois lettres apparues en 1977, sur lesquelles on trouvera d'autres renseignements dans le chapitre sur mathématiques et informatique, furent le signal d'un renouveau d'intérêt atteignant jusqu'aux milieux militaires pour ces deux problèmes, presque aussi vieux que notre discipline. Depuis, ils n'ont pas quitté le devant de la scène.

Il y a deux manières, toutes deux très anciennes, de dresser des listes exhaustives de tous les nombres premiers compris, disons entre 2 et 10 000 000. La première porte le nom de crible d'Ératosthène. Avec l'étendue que nous nous sommes fixée, elle semblerait inapplicable puisqu'il s'agit d'écrire côte à côte les entiers de 2 à 10 000 000, de barrer tous les multiples de 2 autres que 2, puis tout les multiples de 3 — plus petit entier non barré supérieur à 2 — autres que 3, et ainsi de suite. C'est impossible sur un cahier d'écolier, mais praticable à l'intérieur de mémoires d'ordinateur. Ce qui reste vierge fournit la réponse. Il en existe des variantes amusantes, comme celle de Matiassevitch (voir page 33 de la bible des *Merveilleux Nombres premiers* de Jean-Paul Delahaye, Belin).

La seconde méthode est plus facile à mettre en œuvre, mais moins spectaculaire. Elle consiste, dans sa version la plus grossière, à tenter de diviser tous les entiers n

de 2 à 10 000 000 par tous les entiers $m < \sqrt{n}$ et à ne garder que ceux qui ont résisté à toutes ces divisions. On peut l'améliorer en décidant de commencer par un crible d'Ératosthène, disons jusqu'à 5 ou 19, mais l'écriture et l'exécution du programme réalisant l'algorithme se compliquant vite inutilement, il vaut mieux rester rustique. Cela marche très bien : n'importe quel possesseur de PC peut se faire sa petite banque de cette façon, et l'offrir à sa famille pour les fêtes de fin d'année.

Le problème connexe est la décomposition en facteurs premiers. Inutile de décrire ici comment s'y prendre ; il s'agit pratiquement des essais successifs que l'on vient de voir.

Tel était en tout cas l'état de l'art pendant de nombreux siècles, même si des avancées importantes avaient été faites par des chercheurs géniaux comme l'inévitable Fermat, partant pourtant de la banale identité algébrique $x^2 - y^2 = (x - y)(x + y)$. Les nécessités de la cryptographie moderne poussant, les progrès en géométrie aidant, la puissance des ordinateurs grandissant, de toutes nouvelles méthodes ont vu le jour, surtout depuis 1980 voire 1990, à base de courbes elliptiques par exemple, qui ont bouleversé le paysage. Cela dit, factoriser reste sans doute un problème *difficile*, en un sens très précis que nous ne pouvons malheureusement développer ici. La recherche continue, plus vivante que jamais.

À ces problèmes on peut relier le suivant : dire si un nombre donné est premier ou non, sans chercher de décomposition ; et encore celui-ci : répondre à la question précédente non de manière complètement déterministe, mais seulement avec une probabilité d'erreur très proche de 0. Nous disposons aujourd'hui de moyens tout à fait surprenants pour répondre à ces questions, avec une très grande vitesse même pour de longs nombres (voir n'importe quel logiciel de calcul formel comme Mathematica, et surtout le très complet livre de Delahaye).

Le problème d'Euclide (330-275)

Qu'est-ce qu'une parallèle ?

L'axiomatique d'Euclide a ouvert la porte à toutes les autres. Qu'est-ce qu'une démonstration ? Est-ce utile ou nécessaire ? Notre chapitre sur la géométrie est entièrement consacré à cette passionnante construction abstraite de l'esprit sur la base la plus concrète qui soit, dont les derniers (?) échos marquèrent la fameuse querelle des mathématiques « modernes ».

Pour beaucoup, la géométrie est le symbole même des mathématiques. Son histoire prestigieuse paraît peut-être terminée, mais grâce à une sortie par le haut d'une exceptionnelle grandeur : tout mathématicien moderne, quelle que soit sa technicité, reconnaît qu'il fait tous les jours de la géométrie, même si ses « figures » sont parfois bien virtuelles. Euclide n'est pas près de mourir.

Le problème d'Eudoxe (408-355)

Les grandeurs sont-elles mesurables ?

Dans cette première ébauche de la notion de nombre réel se profile le monde fascinant des encadrements, approximations diverses (fractions continues, écriture des nombres), donc toute l'analyse classique, mais aussi toute l'analyse numérique de notre siècle et, plus généralement, ce que l'on appelle les mathématiques « appliquées » qui, contrairement à un préjugé tenace, ne sont pas les moins rigoureuses même si leur utilisation par d'autres est parfois trop imprudente.

Notre chapitre sur les nombres s'ouvrira donc sur Eudoxe, l'un des mathématiciens grecs les plus originaux et les plus féconds, inspirateur d'Euclide et peut-être l'égal d'un Archimède.

Le problème d'Euler (1707-1783)

Y a-t-il dans cette salle quelque chose à calculer ?

Il y en a tant, de problèmes inventés et traités par Leonhard Euler, que le choix est très difficile ! Aussi nous en tirerons-nous par une pirouette. Euler restera dans ce panorama comme le représentant le plus doué et le plus fécond de tout un siècle qui vit l'explosion des conséquences des idées nouvelles issues du prodigieux XVII^e siècle.

Il n'y a pas de sujet qu'Euler n'ait touché. En théorie des nombres, il démontra le premier les principales propositions de Fermat, peu soucieux de publication, marquant même des points dans le domaine difficile du « grand théorème ». En analyse surtout, il lança ses formidables capacités de calculateur sur toutes les pistes : équations différentielles, séries, géométrie différentielle, fonctions complexes... Ses œuvres complètes ne sont même pas encore totalement publiées. Si son manque de rigueur peut lui être reproché à juste titre, il pourrait se défendre en se repliant derrière l'incitation de Pascal à prier d'abord, refuge de tous ceux qui préfèrent l'exploration intrépide de terres inconnues à la production mesurée de résultats sûrs.

L'histoire étrange de la succession de ces deux périodes palpitantes, de 1600 à 1700, puis de 1700 à 1800, constitue le meilleur exemple de ce qu'est la dialectique mathématique fondamentale : on *inspire* en ouvrant de nouvelles voies comme le calcul différentiel et intégral, puis on *expire* en résolvant des problèmes jusqu'alors impensables ou inabordables. Plus l'on se rapproche de nos jours, plus l'étendue de ces différentes périodes se raccourcit ; le XX^e siècle a vu se dérouler les deux temps successifs en son sein. Le statut du XXI^e est encore inconnu. Peut-être verra-t-il — par exemple à partir de la considération de mailles de dimension n de réseaux — des novations aussi exceptionnelles qu'entre 1630 et 1680 ; ce n'est pas absolument certain. On peut être sûr que les émules d'Euler ne manqueront pas.

Le problème de Fermat (1601-1665)

La plus célèbre équation diophantienne.

Déjà aux dires de Proclus (412-485) Pythagore avait su résoudre, au moins partiellement, une équation diophantienne (du nom de Diophante, de beaucoup son cadet), c'est-à-dire une équation de la forme $f(x,y,z) = 0$ où f est un polynôme à coefficients entiers (dans \mathbb{Z}), et où les solutions (x,y,z) sont elles-mêmes à rechercher dans \mathbb{Z} ou dans \mathbb{N} .

Le polynôme f de Pythagore était $x^2 + y^2 - z^2$. Il ne s'agissait bien sûr alors que de racines positives, à savoir (sous forme modernisée) : $(x,y,z) = (2n + 1, 2n(n + 1), 2n^2 + 2n + 1)$ où n est un entier arbitraire, c'est-à-dire encore $\left(m, \frac{m^2 - 1}{2}, \frac{m^2 + 1}{2}\right)$ où m est impair. Il existe d'autres familles de solutions, dont

bien entendu $(x,y,z) = (2n, n^2 - 1, n^2 + 1)$, soit encore $\left(m, \frac{m^2}{2} - 1, \frac{m^2}{2} + 1\right)$ où m est pair, attribuée cette fois-ci à Platon par Proclus, les triplets de Pythagore s'obtenant en divisant ceux-là par 2 lorsque n est impair.

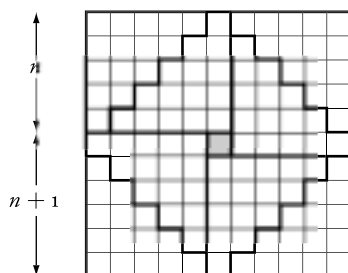
Il n'est pas trop difficile de voir que les solutions générales, bien plus nombreuses, sont à un éventuel échange de x et y près, de la forme, parfois dite « indienne », $x = w(u^2 - v^2)$, $y = 2uvw$ et $z = w(u^2 + v^2)$, où (u,v,w) sont des entiers positifs arbitraires, à ceci près encore que l'on doit prendre $u \geq v$ (on retrouve Pythagore en posant $u - v = w = 1$).

Ces formules ont une histoire embrouillée. Elle figurent déjà (sans w) dans le livre X des *Éléments* d'Euclide, avec démonstration — voir notre chapitre sur les nombres —, mais aussi dans les *Subasûtras* indiens, peut-être contemporains de Pythagore. Le problème était bien entendu interprétable sous forme géométrique : trouver tous les triangles rectangles à côtés entiers, depuis appelés triplets pythagoriciens. Elles étaient même probablement déjà connues des Babyloniens d'avant 1900 av. J.-C. (voir la célèbre tablette Plimpton 322).

Beaucoup de personnes, même cultivées, sont toujours étonnées d'apprendre que Platon, connu surtout comme philosophe, était sans doute aussi un mathématicien, probablement pas original mais en tout cas capable de reconnaître et de diffuser des résultats intéressants. Il en va de même pour l'historien Plutarque (49-125), à qui l'on devrait l'observation selon laquelle ajouter 1 au produit par 8 d'un nombre triangulaire, donc de la forme $\frac{n(n+1)}{2}$, donne un carré.

Le théorème de Plutarque

Une démonstration algébrique de cette proposition est immédiate, si l'on sait sommer les suites arithmétiques (et la plus simple d'entre elles, à savoir $1 + 2 + \dots + n$); la légende veut que Gauss ait compris comment le faire alors qu'il n'était encore qu'un écolier (il suffit de doubler cette somme en ajoutant 1 à n , 2 à $n - 1$ et ainsi de suite). Une démonstration géométrique directe redonne ce résultat, en s'appuyant sur huit pseudo-triangles, qui justifient le nom de « nombre triangulaire » donné aux sommes d'entiers consécutifs à partir de 1 :



$$8(1 + 2 + \dots + (n - 1) + n) + 1 = (2n + 1)^2$$

figure 33. Le théorème de Plutarque

On peut même lire sur ce dessin, qui rappelle les démonstrations imagées du théorème de Pythagore, que le carré annoncé n'est autre que celui de $n + (n + 1) = 2n + 1$. On peut d'ailleurs généraliser facilement ce théorème en utilisant la même idée géométrique à partir de huit pseudo-trapèzes entourant un carré.

S'il n'est pas trop difficile de retrouver la méthode des Babyloniens, il faut être nettement plus habile pour étudier de même les *triangles cartésiens* définis, portant le nom d'un autre littéraire, par les polynômes $f = x^2 - xy + y^2$ et $f' = x^2 + xy + y^2$. Il en donne des racines sous forme paramétrique, à la suite d'une présentation des triplets pythagoriciens et absolument sans justification, dans des documents retrouvés et publiés après sa mort connus sous le nom d'*Excerpta* (extraits). Les formules de Descartes ne donnent, apparemment, pas toutes les solutions, mais on les généralise très facilement (se reporter aux *Œuvres complètes* de Descartes en cours de réédition à la Pléiade, et à notre chapitre 7 sur les nombres).

L'équation de Fermat

Après Diophante, qui d'ailleurs acceptait aussi bien les racines rationnelles que les entières dans une œuvre passionnément redécouverte et étudiée aux xvi^e et $xvii^e$ siècles notamment par Descartes comme on l'a vu, c'est évidemment Fermat qui reprend le flambeau. Il résout certaines questions difficiles — comme $x^3 - y^2 - 2 = 0$, qui n'a qu'une seule solution (3,5) — mais surtout pose une énigme directement issue de Pythagore : quels sont les triplets vérifiant $x^n + y^n - z^n = 0$ où n est supérieur ou égal à 3 ? Il est bien connu qu'il avait affirmé vers 1637 qu'il ne pouvait y avoir de solution en entiers non nuls ; il en avait effectivement la preuve au moins pour $n = 4$. Cela dit, même si Euler et bien d'autres ont apporté au fur et à mesure des confirmations pour des cas particuliers, le dénouement de cette énigme attendra 1994 et les célèbres huit années de travail solitaire d'Andrew Wiles (né en 1953, donc juste trop tôt pour pouvoir espérer une médaille Fields inexorablement fermée aux plus de quarante ans).

Ce qu'il y a d'intéressant dans cette démonstration, qui mérite des ouvrages à elle seule (voir par exemple un autre livre de Simon Singh, mais surtout, à un niveau plus élevé, Yves Hellegouarch, *Les Mathématiques de Fermat-Wiles* chez Masson, écrit par un précurseur de la victoire finale), c'est qu'elle a nécessité toute une foule d'étapes intermédiaires et d'intuitions géniales, dont certaines de nos compatriotes Hellegouarch déjà cité, Jean Pierre Serre et évidemment le grand André Weil. C'est aussi que la première version présentée au public en 1993 était fautive, qu'il avait fallu six mois pour que le monde scientifique s'en persuade et un an pour que l'auteur, venant recréer une voie latérale trop vite abandonnée, puisse réparer les lacunes de son premier manuscrit.

Cette histoire est dédiée à tous ceux qui pensent qu'une démonstration mathématique n'est qu'un exercice médiocre, dont on pourrait laisser la vérification à quelques spécialistes, pourquoi pas à des ordinateurs de haut de gamme...

Le problème de Fourier (1768-1930)

Comment réchauffer l'eau du bain ?

Le préfet de l'Isère Joseph Fourier est à l'origine du déchiffrement des hiéroglyphes, puisqu'il fit parvenir à son jeune protégé Jean-François Champollion une copie de la pierre de Rosette. À Grenoble, les rues Fourier et Champollion sont d'ailleurs dans un prolongement symbolique clair, dont le sens doit échapper à quelques badauds.

Cela dit, l'ancien égyptologue bonapartiste est surtout célèbre pour avoir, le premier, osé attaquer le problème de la chaleur, prototype avec celui du télégraphiste et quelques autres, des équations aux dérivées partielles qui gouvernent la nature.

Les séries qui portent son nom sont aussi liées à l'étude des cordes vibrantes qui remonte à l'Antiquité et a passionné Euler et bien d'autres. Pour les physiciens, Fourier a été l'un des maîtres qui leur ont ouvert la porte du monde. D'ailleurs il est parfois considéré comme l'un des leurs.

L'analyse de Fourier, que nous ne pouvons qu'évoquer par cette très brève note, est toujours vivante ; les ondelettes d'Yves Meyer (partant de travaux d'ingénieurs ayant flairé là quelque chose d'important, comme Heaviside, enfin réhabilité en 1944 par Laurent Schwartz) n'en sont que le dernier avatar. Il est donc à parier que l'on n'a pas fini d'entendre parler de l'un de ceux qui ont pu montrer l'importance décisive du calcul différentiel et intégral dans la découverte des secrets de la nature.

Le problème de Galilée (1564-1642)

Comment tombent les corps ?

Il était exclu de ne pas citer ici, sous une forme ou une autre, le point de départ de la physique mathématique, illustre fille des mathématiques, qui n'a peut-être pas complètement quitté les jupes de sa mère. De nombreux chercheurs théoriciens ne se refusent-ils pas à choisir entre les deux disciplines ?

Galilée est à la fois un astronome, un physicien expérimental, un inventeur d'appareils scientifiques, un théoricien et aussi un mathématicien, comme on le voit par son célèbre paradoxe sur l'infini — il y a autant de nombres pairs que de carrés parfaits — et ses recherches sur certains compas, ou surtout sur l'oscillation du pendule simple où il introduit la notion de calcul comme outil capital de la science. Il était certes capable d'un grand pragmatisme, par exemple en recourant à des expériences pour déterminer des aires, mais ses livres de philosophie des sciences montrent qu'il avait été capable de faire une synthèse personnelle remarquable des connaissances de son temps. Il mérite d'être considéré comme le premier en date de toute la galerie impressionnante des grands scientifiques qui marqueront l'immense XVII^e siècle.

Le problème de Galois (1811-1832)

Résoudre les équations algébriques.

Étant donné un polynôme P , déterminer les nombres réels (éventuellement complexes) tels que $P(x) = 0$. Un Descartes croyait, pensons-nous, que c'était là la question la plus importante au monde ; arrivé à une époque où l'on savait résoudre — par radicaux — les cas où P était de degré au plus quatre, grâce par exemple aux antiques Babyloniens (2000 av. J.-C. ?) et aux Italiens du XVI^e siècle, de Scipione del Ferro (1465-1526) à Tartaglia (1499-1557), Cardan (1501-1576), Ferrari (1522-1560) et Bombelli (1526-1573), il avait cru mettre au point une technique générale de résolution par intersections d'un cercle et de courbes algébriques.

Après lui, Gauss montrera que toute équation complexe non triviale a au moins une racine, mais c'est à Évariste Galois que revient l'immense mérite d'éclaircir complètement, à vingt ans, l'épineuse question de savoir pour quel type de polynôme une résolution par radicaux est possible. Peu de temps auparavant, Niels Abel (1802-1829) avait démontré, à vingt-deux ans, que l'équation générale du cinquième degré ne rentrait pas dans ce cadre.

Galois a aussi jeté les bases de l'algèbre moderne, indiquant comment construire des sur-corps de corps donnés où un polynôme de degré n possède exactement n racines. Le 16 octobre 1843, Hamilton gravera sur le parapet du Brougham Bridge de Dublin les formules de base du calcul des quaternions qu'il vient de découvrir, en se rendant au bras de son épouse à une séance de l'Académie royale irlandaise. Il faudra attendre 1944 pour qu'un théorème à la d'Alembert puisse être démontré pour les polynômes quaternioniens par Samuel Eilenberg et Ivan Niven, mettant peut-être le point final à une histoire qui a duré quatre mille ans.

Le problème de Gauss (1777-1855)

Construire un polygone régulier à la règle non graduée et au compas.

L'œuvre de Carl Friedrich Gauss est immense. Citons pêle-mêle : la découverte à dix-neuf ans (le 30 mars 1796) que le polygone régulier à 17 côtés est constructible à la règle non graduée et au compas parce que 17 est un nombre de Fermat (ainsi peut-on construire le côté d'un polygone ayant 257 côtés ; une valise contenant les détails d'une construction pour 65 537 côtés traînerait à l'université de Göttingen) ; la *loi de réciprocité quadratique* sur une condition nécessaire et suffisante pour qu'un nombre premier p soit congru à un carré parfait modulo un autre nombre premier q ; le théorème de d'Alembert-Gauss, qui dit que tout polynôme non constant admet

Ce théorème d'incomplétude de Kurt Gödel élaboré en 1931 a été enrichi en 1938 par la première étape de la preuve que l'axiome du choix de Zermelo et l'hypothèse du continu de Cantor sont justement des cas particuliers de telles propositions indécidables. Elles ne sont pas les seules contributions de ce mathématicien hors norme. Le résultat, basé sur une variante excessivement subtile du procédé diagonal de Cantor appuyé sur les « nombres de Gödel », ruina les certitudes de Hilbert quant à une preuve de non-contradiction des mathématiques dont il rêvait.

Gödel a aussi démontré en 1930 un autre théorème d'incomplétude après avoir commencé sa vie universitaire, en 1929, par un théorème de consistance. Il est également connu comme ayant participé à la mise sur pied d'un système d'axiomes pour la théorie des ensembles, ce qui peut paraître étrange compte tenu de son principal résultat. Philosophes et journalistes se saisirent encore longtemps de ce théorème d'existence de propositions ni démontrables ni réfutables pour moquer gentiment la prétention, vraie ou supposée, des mathématiciens à gouverner le monde des idées. Qu'ils s'étonnent ensuite de les voir, comme sur la fresque de Puvis de Chavannes, leur tourner rageusement le dos ?

Le problème de Grégoire XIII (1502-1585)

Astronomie et calendrier.

En 45 av. J.-C., Jules César, notant que l'année solaire était plus proche de 365 jours $\frac{1}{4}$ que de 366 jours $\frac{1}{4}$, créa le calendrier julien avec une année bissextile tous les quatre ans. Mais il n'est pas le seul chef d'État à figurer dans notre palmarès.

L'année moyenne de 365,25 jours adoptée par le calendrier était trop longue. On le comprit avec la constatation de 10 jours d'avance pris après 15 siècles par l'équinoxe de printemps : une commission d'astronomes, dont faisaient notamment partie Clavius et Lilio, constituée par le pape Grégoire XIII, considéra que 365,2425 serait une meilleure détermination. Telle est la valeur que retint la bulle *Inter Gravissimus* du 24 février 1582 décidant qu'à l'avenir les années séculaires seraient bissextiles seulement une fois sur 4, en 1600, 2000, 2400..., de sorte qu'en 400 ans il y aurait 97 années bissextiles au lieu des 100 instaurées par Jules César, quitte à élever la durée du cycle des dates de Pâques de 532 ans à 5,7 millions d'années. Par ailleurs, pour que l'équinoxe de printemps se trouve le 21 mars en 1583, l'idée de supprimer des jours — émise dès le XIII^e siècle par le moine anglais Jean de Halifax dans *De Anni Ratione* — fut retenue. En Italie, le lendemain du jeudi 4 octobre 1582 fut déclaré être le vendredi 15 octobre. Cette neutralisation de dix jours eut lieu la même année en France, entre le 9 et le 20 décembre, et dans les États catholiques des Pays-Bas, entre

le 14 et 25 décembre. Ce fut en 1700 seulement en Allemagne et en Suisse, en 1753 en Grande-Bretagne. L'Église orthodoxe russe a conservé le système julien d'où son décalage avec notre calendrier grégorien — atteignant à l'heure actuelle 13 jours. La Révolution d'octobre en novembre...

On a un peu causé dans les médias de ces problèmes d'arithmétique quotidienne au seuil de l'année mondiale des mathématiques (comme c'est étrange !) d'abord à cause de l'éclipse totale du soleil du 11 août 1999, ensuite par curiosité au sujet du bizarre 29 février 2000, bissextile bien que marquant un virage de siècle (sur fond de risques d'un certain bogue informatique). Mais que l'on se rassure : ces choses-là n'arrivent qu'une fois dans une vie, et l'on n'est pas près d'entendre de sitôt reparler de nombres à la télé.

Le problème d'Hermite (1822-1901)

Quels sont les nombres transcendants ?

Les nombres e , π et les autres... Nous voulons parler ici de la foule, souvent complètement anonyme, des nombres transcendants, qui ne sont racines d'aucune équation à coefficients entiers.

Déjà les rationnels sont très peu nombreux, il est facile de les dénombrer en file indienne ; les algébriques, c'est-à-dire non transcendants, ne sont pas, finalement et en dépit des apparences, plus nombreux que les rationnels, qui forment le sous-corps des nombres algébriques de degré un. Donc il n'y aurait pratiquement qu'à se baisser pour trouver un nombre transcendant.

Et pourtant... Il a fallu attendre 1844 et Joseph Liouville (1809-1882) pour en voir un bien précis, 1893 pour que Charles Hermite (1822-1901) — patron encore vert et tout-puissant des mathématiques françaises de son temps — prouve que l'irrationnel $e = 2,71828\dots$ n'était pas algébrique, tout en renonçant à prouver qu'il en était de même pour π . C'est à Ferdinand von Lindemann (1852-1939), étoile de bien moindre grandeur, qu'est revenu l'honneur de le faire, terminant ainsi une quête multiséculaire de quadrature du cercle.

L'irrationalité de π , évidemment plus facile, avait été prouvée en 1761 par Jean Lambert (1728-1777). Aujourd'hui cette irrationalité pourrait faire l'objet d'un problème de baccalauréat, celle de e d'un exercice de première année de Deug, la transcendance de e d'un problème de seconde année et celle de π d'un examen de licence. Somme toute, il suffisait d'attendre.

Le problème de Hilbert (1862-1943)

Quels seront les problèmes de demain ?

Les vingt-trois problèmes de David Hilbert, présentés à la Sorbonne le 8 août 1900 devant deux cent vingt participants au II^e Congrès international de mathématiques par le pape des mathématiques allemandes (Poincaré défendant la vaincue de 1870), n'étaient pas tous des problèmes au sens précis du terme, mais parfois des indications relativement vagues sur des recherches à venir. Ils ont joué un rôle essentiel pendant tout le XX^e siècle. Pourquoi ?

La mathématique progresse de deux façons : en créant de nouveaux territoires (Descartes, Newton...) et en résolvant des problèmes (Gödel, Matiassevitch, Wiles...). Toute personne relevant l'un des défis de Hilbert a la gloire assurée : il en reste essentiellement trois, dont la formidable conjecture de Riemann. D'autres, comme celle de Fermat, juste citée dans son avant-propos, n'étaient pas dans la liste. Peu importe. L'essentiel est que, une fois la « curiosité » piquée, certains en perdent le sommeil. Lecteurs, à vos ordinateurs ! D'autant plus qu'il y en a maintenant six autres proposés par le Clay Institute...

Hilbert fut un très grand mathématicien, cela est bien connu ; on sait moins que sa distraction était celle, légendaire, du savant. On rapporte qu'un jour le couple Hilbert devant recevoir des invités à dîner, sa femme trouva la chemise de son mari trop sale : elle lui demanda de monter se changer. Des quarts d'heure passèrent, les invités arrivèrent ; Mme Hilbert, inquiète, monta et trouva son mari profondément endormi, la séquence des gestes qu'il avait exécutés pour enlever sa chemise l'ayant envoyé droit au lit.

Le problème de Kepler (1571-1630)

Qu'est-ce qu'un maximum ?

Johannes Kepler est surtout connu comme astronome, assistant de Tycho Brahe (1546-1601) dont la magnifique tombe orne la cathédrale du Tyn à Prague, et inventeur des trois lois d'où partira Newton pour bâtir son système du monde. L'idée d'utiliser des ellipses, créant au passage le mot « foyer », lui a valu une gloire immortelle. Signalons toutefois au passage qu'il faut qu'un lecteur d'aujourd'hui soit déjà bien averti pour découvrir ces lois dans ses Œuvres complètes (deux dans un livre de 1609 *Astronomia nova*, la troisième dans un autre de 1619, *Harmonices mundi*), et le fameux mot « brûlant » (dans les *Paralipomena ad vitellionem* de 1604), au milieu d'un déluge de propositions du style : on pourrait faire ceci, ou cela et ainsi de suite.

Le métier d'historien des sciences, même à un niveau modeste, demande beaucoup d'obstination. Ainsi, observer dans une première lecture de *La Géométrie* la naissance officielle de ce qui deviendra les coordonnées cartésiennes n'est pas non plus une partie facile (même le plaisir n'est pas toujours gratuit).

Se plonger dans Kepler a pourtant aussi une autre utilité : c'est que certains y ont vu un précurseur du calcul différentiel et intégral. Il est vrai qu'il a calculé pas mal de volumes, surtout pour des tonneaux (dans un but très pratique, puisqu'il s'adressait au monde viticole de sa province autrichienne dans la *Nova stereometria doliorum vinariorum* publiée à Linz en 1615). C'est dans ce livre qu'il écrit également, ce qui est plutôt une remarque au passage que l'amorce d'une idée profonde à exploiter plus tard, que lorsque l'on se rapproche d'un maximum, ici de volumes de parallélépipèdes inscrits dans une sphère, *le changement de ces volumes devient de plus en plus petit*. Certains ont voulu y voir la clef de la méthode *De maximis et minimis* de Fermat, conçue quelque vingt ans plus tard.

Si cette interprétation était vraie, on pourrait imaginer en germe dans ce type de remarque toute l'analyse, et son application à la maîtrise de la nature ; mais c'est sans doute une reconstruction beaucoup trop hasardeuse. Mieux vaut attendre que Newton et Leibniz passent à la pratique.

Par ailleurs, Kepler avait introduit en 1604 (*Astronomia pars optica*) une première idée de l'infini en arguant que le second foyer d'une parabole existe bien, mais au-delà de toute distance, puisque cette conique peut être obtenue comme limite d'une ellipse qui s'étire, avant de devenir enfin hyperbole. Apollonius et lui ont dû avoir, dans l'au-delà — Kepler était très croyant —, de bien passionnantes conversations.

Le problème de Lebesgue (1875-1941)

Comment trouver l'intégrale universelle (ou presque...)?

La longue histoire des différentes étapes du concept d'intégrale passe par les noms prestigieux de Newton, Leibniz, Cauchy, Riemann, Denjoy, Perron, Kurzweil, Henstock, Mac Shane... et surtout Henri Lebesgue qui, le 29 avril 1901, deux cent trente-cinq ans après Newton, quatre-vingts ans après Cauchy, quarante-sept ans après Riemann, dépose à l'Académie des sciences un compte rendu où il propose une nouvelle notion, la *sommabilité* (aujourd'hui intégrabilité) qui permet de définir de façon beaucoup plus cohérente les notions de longueur, d'aire et de volume.

En fait c'est toute l'analyse qui est bouleversée. De grands mathématiciens contemporains pensent, un siècle plus tard, que l'intégrale de Lebesgue ne sera jamais délogée de son piédestal, au moins dans un avenir prévisible.

Pourtant il reste aujourd'hui un vrai problème : comment enseigner cette intégrale, qui passe toujours pour délicate auprès des étudiants, et qui doit souvent être « préparée » par une présentation plus ou moins poussée des vieilles intégrales de Cauchy ou de Riemann, plus faciles à introduire et qui, il est vrai, avaient parfaitement suffi à un Henri Poincaré. En mathématiques, les questions de pédagogie ne sont pas toujours *négligeables*. Il est possible que cette situation finisse par se débloquer, ce qui permettrait aux scientifiques non spécialistes — physiciens, ingénieurs — de pouvoir se servir sans restriction d'un instrument incomparable.

Le problème de Legendre (1752-1833)

La répartition des nombres premiers obéit-elle à une loi simple ?

Adrien-Marie Legendre, puis Gauss ont longtemps soupçonné que le nombre de nombres premiers inférieurs à x était donné, avec une très bonne précision, par la formule $\pi(x) = \frac{x}{\ln x}$. Le second avait même proposé une valeur, équivalente à la précédente, mais encore plus précise à l'aide d'une primitive de la fonction définie par $\frac{1}{\ln x}$. On en déduit que le nombre premier de rang n est approximativement donné par l'égalité $p_n = n \ln n$ où la fonction \ln représente bien entendu le logarithme népérien.

Ces intuitions basées sur quelques idées simples mais surtout sur les tables existantes, confortées par des travaux importants de 1849 et 1851 de Pafnouty Tchebitcheff (1821-1894), ne furent confirmées qu'en 1896, et indépendamment, par Jacques Hadamard (1865-1963) et Charles de La Vallée-Poussin (1866-1962), à l'aide de techniques lourdes d'analyse complexe, mais aussi en 1948 par Pál Erdős (1913-1996) et Atle Selberg (né en 1917), avec un habillage d'algèbre réelle bien plus simple. Notons par exemple que $\pi(10^9) = 50\,847\,534$, alors que l'approximation en $x/\ln x$ est à peu près $48\,254\,942$: le désaccord n'est que de 5%. Il est encore de 3% pour 10^{14} .

Les démonstrations élémentaires de ces deux derniers mathématiciens, ayant voulu tirer chacun de leur côté une preuve où le travail de l'autre soit complètement estompé (!) sont aujourd'hui lisibles par un bachelier. Curieux destin pour un problème qui avait bloqué Gauss, mais a en revanche peut-être contribué à conduire ses deux premiers vainqueurs à un âge honorable de presque cent ans ; notons cependant que la mort plus prématurée d'Erdős a rompu le charme...

Il est piquant de noter que, récemment, des chercheurs français (Patrick Cégielski, Denis Richard, Olivier Sudac) ont obtenu des résultats intéressants sur la possibilité de démontrer le théorème de Gustave Dirichlet (1805-1859) sur les nombres

premiers dans une progression arithmétique et simplifié par Selberg, dans le seul cadre des axiomes de Peano (1988), puisqu'il en va de même de celui de Hadamard et La Vallée-Poussin (1997). Les mathématiques continuent à avancer, même sans ordinateurs, bien après qu'ils envahissent les laboratoires.

Le problème de Mandelbrot (né en 1924)

Quelle est la longueur des côtes de la Bretagne ?

Le mathématicien et informaticien Benoît Mandelbrot, neveu de Szolem Mandelbrojt (1899-1983), a su comment voir (et mettre) de l'ordre dans un chaos qu'il a en grande partie pu découvrir ou retrouver lui-même dans des travaux antérieurs apparemment épars. Car le chaos est partout ! Cet IBM Fellow a su mettre en valeur un univers étrange, grâce auquel certains ont été attirés vers les mathématiques, soit pour raisons de mode, soit grisés par une fascination plus sérieuse.

Les applications des fameuses fractales envahissent bien des domaines ; nous ne citerons que celui de la compression d'images, si important pour le futur proche de l'informatique. Les chercheurs en physique raffolent de ces mathématiques de l'étrange.

Un gag : un journal a prétendu, en 1999, que l'on avait trouvé, tel Newton, la « vraie loi » de l'évolution des espèces animales — rien que ça. D'après l'article, on peut en déduire qu'elle s'écrirait finalement sous la forme très banale : $t_n = g^{-n} t_o + (1 - g^{-n}) t_c$, où n est le nombre d'années depuis l'apparition de l'espèce et t_c un « temps critique », équation décrivant simplement un phénomène de type combinaison barycentrique de deux exponentielles. Mais « exponentiel » sonne vieillot et usé, tandis que l'on fait beaucoup plus sérieux en mettant en exergue le mot magique « fractal ».

Mandelbrot lui-même, pourtant (légitimement) fier de sa percée, ne confond pas une suite simplement répétée d'homothéties de rapports en progression géométrique avec un vrai phénomène comme celui qu'il a su tirer des œuvres de Gaston Julia (1893-1978) ou de ses propres travaux. A-t-il été amusé de cet hommage peu convaincant ? En tout cas, il est trop tôt pour dire ce qui sortira encore de son problème, apparemment si anodin, même si l'on est sûr que tout n'a pas encore été extrait d'une mine qui paraît encore féconde, en liaison forte avec le concept généralisateur de *systèmes dynamiques* qui permet de mieux appréhender nombre de situations complexes du monde d'aujourd'hui.

Le problème de Matiassevitch (né en 1947)

Il n'y a pas d'algorithme permettant de décider si une équation diophantienne admet ou non des solutions.

En 1970, Youri Matiassevitch devient célèbre en résolvant, par la négative, le dixième problème de Hilbert. Comme très souvent, il y parvient par une voie totalement nouvelle, qui lui a permis de créer un champ de recherches personnel de type alors inconnu, et par un emploi étonnant de la suite de Fibonacci. Ses grandes idées sont assez simples pour qu'elles puissent être présentées dans des revues d'étudiants, au lieu d'être réservées à des séminaires spécialisés. Il est bien connu dans notre pays, où il vient souvent.

Outre la gloire qui attendait naturellement toute personne relevant l'un des vingt-trois défis, Matiassevitch a obtenu d'avoir piqué la curiosité d'un grand public en permettant, par le contenu même de sa démonstration, d'affirmer qu'il existait un polynôme à plusieurs variables dont les valeurs positives prises, lorsque l'on se limite à des variables elles-mêmes positives, recouvrent exactement l'ensemble des nombres premiers. (Il en existe plus généralement un pour tout ensemble *diophantien*, dans le vocabulaire qu'il a créé à cette occasion ; les nombres premiers ne jouent pas là un rôle exceptionnel.) En 1976, un tel polynôme, à 26 variables, a été publié pour la première fois. Il est assez beau à regarder, mais perdrait beaucoup de son charme si l'alphabet latin ne suffisait plus pour l'écrire !

Le problème de Ménechme (IV^e siècle av. J.-C.)

À quoi servent les coniques ?

Les mathématiques « utiles » n'existent pas. L'invention, ou plutôt la découverte, si l'on est platonicien, des coniques par Ménechme, élève d'Eudoxe, sans doute pour résoudre le problème de la duplication du cube en coupant deux paraboles de même sommet et d'axes orthogonaux (ou une parabole et une hyperbole), leur exploitation jusqu'à engendrer la somme apollonienne *pour le seul plaisir de l'esprit*, conduisirent presque vingt siècles plus tard à un retournement de situation exceptionnel. Dans les mains de Kepler, les coniques, objets abstraits par excellence, devenaient les outils nécessaires de la découverte de lois de la nature jusque-là inconcevables.

Ce contre-exemple sur l'importance d'une recherche désintéressée, libre, face aux demandes pressantes d'une société avide de rendement à terme visible, devrait être plus souvent exploité par les responsables de l'éducation et de la recherche. Il en

est d'autres (le calcul matriciel récupéré par Einstein...) qui devraient aussi inviter à la prudence en matière de prospective scientifique.

Autres paradoxes étonnants : il a fallu attendre 1639 et le concept de pôles et polaires de Girard Desargues (1591-1661), 1814 et les théorèmes sur les couples de tangentes aux coniques du prisonnier de guerre Jean-Victor Poncelet (1788-1867), 1822 et les « théorèmes belges » de Germinal Dandelin (1794-1847) et Adolphe Quételet (1796-1874) pour parfaire la théorie purement géométrique des sections planes d'un cône de révolution. Ces théorèmes étaient autrefois un point exceptionnel des programmes des classes terminales dites de mathématiques « élémentaires » ou « supérieures ». Rien n'aurait pu empêcher Euclide de les découvrir. Une longue patience est parfois nécessaire pour être en droit d'affirmer qu'une théorie mathématique est close...

Nous ne pouvons pas ne pas signaler que le sort étrange des coniques a été suivi par leurs cousines germaines les cubiques, ou du moins certaines d'entre elles (les *courbes elliptiques*) sur l'ensemble des points desquelles on peut définir une loi de groupe déjà considérée par Carl-Gustav Jacobi (1804-1851) en 1834 dans son *De usu theoriae integralium ellipticorum et integralium abelianorum in analysi diophantæ*. On peut même remonter jusqu'aux formules de doublement de l'arc de lemniscate du comte de Fagnano (1682-1766) en 1716, puis d'Euler en 1751 qui en déduisit une formule générale d'addition. Nous avons déjà vu que ces courbes pouvaient servir aujourd'hui pour factoriser de grands entiers, mais leur véritable entrée dans le quotidien d'un très banal Monsieur Toulemonde est pour demain matin.

Voici, traduite en notations modernes, la formule de Fagnano :

$$2 \int_0^x \frac{dt}{\sqrt{1-t^4}} = \int_0^{2x\sqrt{1-x^4}/(1+x^4)} \frac{dt}{\sqrt{1-t^4}},$$

à rapprocher de la formule classique équivalente à l'égalité $\sin 2\theta = 2 \sin \theta \sqrt{1 - \sin^2 \theta}$ pour θ entre 0 et $\pi/2$:

$$2 \int_0^x \frac{dt}{\sqrt{1-t^2}} = \int_0^{2x\sqrt{1-x^2}} \frac{dt}{\sqrt{1-t^2}}.$$

La formule d'addition d'Euler est plus complexe et nous ne la donnerons pas ici ; elle généralise la relation trigonométrique bien connue sur le sinus d'une somme, qui s'écrit sous la forme intégrale :

$$\int_0^x \frac{dt}{\sqrt{1-t^2}} + \int_0^y \frac{dt}{\sqrt{1-t^2}} = \int_0^{x\sqrt{1-y^2} + y\sqrt{1-x^2}} \frac{dt}{\sqrt{1-t^2}}.$$

Au moment de la sortie de ce livre, on annonce que la cryptographie à clefs publiques à l'aide de courbes elliptiques, découverte indépendamment en 1986 par Noel Koblitz et Victor Miller, équipera les téléphones portables de demain. Les mathématiques « gratuites » mettent parfois longtemps à devenir « utiles », mais on voit qu'il n'est pas rare que les spéculations les plus abstraites finissent par quitter les cabinets obscurs des universités pour venir atterrir, sous forme parfaitement concrète, jusque dans nos cuisines...

Le problème de Newton (1642-1727)

Comment retrouver un mouvement à partir de la connaissance des vitesses instantanées ou des accélérations.

Tout un chapitre de ce livre est consacré à ce grand bouleversement, auquel il ne faut naturellement pas oublier d'associer Leibniz, qui partage la gloire de l'invention et de la mise au point du calcul différentiel et intégral. Notons cependant qu'il est second en date de quelque dix ans, même si personne ne nie plus aujourd'hui qu'il soit arrivé à cette découverte de manière indépendante, et que ses motivations n'étaient pas tournées vers des équations différentielles issues de la mécanique pour expliquer le monde, mais de préoccupations plus abstraites, que l'on dirait maintenant plus algébriques.

Contentons-nous de poser ici le problème : à la différence de tous leurs précurseurs d'Archimède à Fermat, Newton et Leibniz ont été capables de fournir des algorithmes de calcul efficaces pour une très large catégorie de problèmes, et non seulement ceux d'un certain type. D'autre part, ils ont créé de toutes pièces un nouvel univers, non pas parce qu'ils ont su résoudre *le problème des tangentes* (définir et déterminer, au moins théoriquement, la tangente en un point quelconque d'une courbe quelconque), non pas parce qu'ils ont su résoudre *le problème des aires* (par exemple calculer, au moins théoriquement, l'aire comprise entre trois segments de droites et une courbe, ou un volume, ou trouver un centre de gravité), mais parce qu'ils ont compris comme personne avant eux que ces deux problèmes, célèbres depuis l'Antiquité, étaient de manière surprenante *les deux volets opposés d'un même processus*. Et des algorithmes performants existaient pour les résoudre, applicables de la même manière à toutes sortes de fonctions, qu'elles soient algébriques (fonctions rationnelles) ou transcendentes (trigonométriques, exponentielles, logarithmiques...).

De plus Newton, par l'importance qu'il a donnée à la notion de développement en série entière et à son application aux équations différentielles de la cinématique, a eu une influence très grande sur la mathématisation de la physique. Même son

système et ses notations ont été bien plus malcommodes à utiliser que l'appareil leibnizien.

Retenons simplement que les années 1665 (Newton) et 1675 (Leibniz) — ces dates sont et resteront approximatives, ne serait-ce que parce qu'une découverte de cette taille n'est ni effective ni maîtrisée en un jour — ont été déterminantes dans le combat de l'homme pour comprendre l'Univers.

Le problème de Pappus (IV^e siècle)

Qu'est-ce qu'un lieu géométrique ?

Il y a plusieurs problèmes connus sous ce nom. Descartes en citera deux dans son livre séminal *La Géométrie* ; nous voulons parler ici du premier, qui lui a servi pour définir, parallèlement à Fermat et indépendamment de lui, la géométrie analytique en 1637, qui elle-même ouvrira, par exemple, la porte à la physique mathématique mais aussi à la géométrie algébrique.

La portée de ce problème est donc forte. Son énoncé était pourtant anodin : étant données $2n$ droites, quel est le lieu géométrique d'un point dont les produits des distances aux n premières reste dans une proportion donnée au produit des distances aux n dernières ?

Les anciens savaient que, pour $n = 2$, il s'agit d'une conique. Descartes le démontre, et c'est le premier cours de géométrie analytique partant d'une équation donnée (ici $D_1 D_2 = k D_3 D_4$) pour remonter jusqu'aux équations « réduites » à la Apollonius. On ne peut qu'applaudir l'artiste, car c'est pour l'époque un tour de force inouï.

Bien sûr, pour d'autres valeurs plus grandes, il ne s'agissait pas de courbes connues, mais Descartes, par un prodigieux retournement du problème, s'en sert justement *comme instrument de création de nouvelles courbes*, de degrés arbitrairement grands, et ouvre la voie à un monde vierge sans lequel la compréhension de notre univers serait restée bien terne et quasiment toute verbale.

Peut-être Descartes a-t-il cru que toute courbe avait une équation « à la Pappus » : on sait aujourd'hui que c'est inexact. Détail piquant : on ignore apparemment si les fameuses Ouales qu'il a définies, pour régler une question fondamentale d'optique, en ont une ou non. Ce serait un beau pied-de-nez posthume de prouver qu'il n'en est rien, mais pas très gentil, après le travail qu'il a donné aux mathématiciens pour au moins une dizaine de siècles.

Le problème de Pascal (1623-1662)

Jouer aux dés n'est pas forcément perdre son temps.

Ce problème et le suivant introduisent dans deux mondes assez particuliers, intimement liés. Il s'agit ici du calcul des probabilités (créé lors d'une correspondance célèbre avec Fermat à partir de questions d'un certain chevalier de Méré, mais surtout pour l'honneur de l'esprit humain). L'implication des mathématiques dans les sciences sociales, mais aussi en biologie et bien d'autres secteurs, est étroitement liée à toutes ces mathématiques appliquées où le hasard a sa place.

C'est bien connu. On sait moins que les probabilités — à la différence des statistiques restées plus proche du concret — jouent aussi un rôle très important en mathématiques pures. Non seulement certains de leurs chapitres sont devenus partie prenante d'une théorie très abstraite (la mesure et l'intégration), mais il existe même des théorèmes sans lien apparent avec l'aléatoire qui ont été démontrés grâce à elles, par exemple en théorie des nombres, où le nom d'Erdős doit absolument être évoqué. Le hasard, domestiqué, se mue parfois en outil de la nécessité...

Quelques résultats paradoxaux en calcul des probabilités

Certains problèmes d'allure innocente ont parfois des solutions qui choquent le bon sens. L'intuition n'est pas toujours commode à mettre en œuvre dans ce domaine. Parmi mille exemples, nous en avons pris deux, respectivement extraits des épreuves de Concours général des années 1999 et 2000.

Le premier problème est le suivant :

Sur une table trônent 1999 bonbons rouges et 6661 bonbons jaunes rendus indiscernables par des emballages uniformes. Un gourmand applique jusqu'à épuisement du stock l'algorithme ci-dessous :

(a) s'il reste des bonbons, il en tire un au hasard, note sa couleur, le mange et va en (b) ;

(b) s'il reste des bonbons, il en tire un au hasard et note sa couleur :

– si elle est la même que celle du dernier bonbon avalé, il le mange et retourne en (b) ;

– sinon, il le remmaillote, le pose et retourne en (a).

Montrer que tous les bonbons seront mangés et donner la probabilité pour que le dernier bonbon mangé soit rouge.

Puisqu'il existe beaucoup plus de bonbons jaunes que de rouges, il semblerait que cette probabilité soit inférieure à 0,5. Or il n'en est rien, et la réponse est 1/2 quels que soient les nombres de bonbons. Ce résultat d'apparence paradoxale peut s'établir par d'assez longs calculs, avec des récurrences numériques

pénibles, en étudiant la probabilité $P(a, b)$ de l'événement R : « le dernier bonbon mangé est rouge » en fonction des effectifs a et b des bonbons de chaque couleur (on définit de même J en échangeant jaune et rouge).

Il en existe aussi une solution bien plus rapide, due à Pierre Douillet, que nous allons esquisser ici. Elle consiste à remarquer d'abord que la description d'une telle expérience gourmande se ramène à la considération d'un nombre fini n de séquences S_1, S_2, \dots, S_n où $2 \leq n \leq 6661 + 1999$. Chaque séquence est associée à une couleur, alternativement jaune et rouge ; elle correspond bien entendu à une dégustation consécutive de bonbons de la même couleur, débutant en un passage en a) et se terminant à la fin d'un b) — il peut d'ailleurs y avoir plusieurs passages par a) au cours d'une même séquence.

Chaque séquence peut être caractérisée par les effectifs initiaux r et j des bonbons de chaque type ; à la fin ces effectifs sont devenus, selon le cas, r et j' avec $j' < j$, ou r' et j avec $r' < r$. La dernière séquence est clairement reconnue à ce que l'un des deux nombres r ou j , et un seulement, est nul. Ainsi l'événement R correspond à $r > 0$ et $j = 0$ au début de S_n ; la séquence précédente S_{n-1} est donc associée à des entiers r et j tous deux non nuls, qui deviennent r et 0 à la fin.

Nous pouvons maintenant introduire l'événement A_n : « n est l'indice de la dernière séquence S_n de l'expérience ». On dispose évidemment de l'égalité $P(A_n) = P(R \cap A_n) + P(J \cap A_n)$ (formule des probabilités totales). L'idée centrale consiste à conjecturer, à la suite d'expérimentations sur de petits entiers, que la probabilité conditionnelle $P(R | A_n)$ (probabilité de l'événement R sachant que l'événement A_n est réalisé) est toujours égale à $1/2$ quel que soit n et quels que soient les effectifs r et j au début de l'avant-dernière séquence S_{n-1} .

En effet un calcul élémentaire montre que la probabilité $P(R \cap A_n)$ de l'événement consistant au passage de (r, j) à $(r, 0)$ lors de S_{n-1} est égale à :

$$P(R \cap A_n) = \frac{j}{r+j} \frac{j-1}{r+j-1} \cdots \frac{1}{r+1} = \frac{j!r!}{(r+j)!} = \frac{1}{C_{r+j}^j}.$$

Elle est donc égale à $\frac{1}{C_{j+r}^r} = P(J \cap A_n)$. Il en résulte que ces deux probabi-

lités sont égales entre elles, d'où $P(R | A_n) = \frac{P(R \cap A_n)}{P(A_n)} = \frac{1}{2}$ par définition d'une probabilité conditionnelle, ce que nous voulions démontrer. Pour pouvoir conclure, il suffit maintenant d'écrire l'égalité (finie en dépit des apparences) :

$$P(R) = \sum_{n=2}^{+\infty} P(R \cap A_n) = \sum_{n=2}^{+\infty} P(R | A_n) P(A_n) = \frac{1}{2} \sum_{n=2}^{+\infty} P(A_n) = \frac{1}{2}.$$

Le second problème est également assez surprenant :

On dispose de b boules blanches et n boules noires — au moins une de chaque —, que l'on répartit entre deux urnes de façon qu'aucune d'elles ne soit vide ; on note s le nombre de boules dans la première, et r celui de ces boules qui sont blanches.

L'évènement considéré est le tirage d'une boule au hasard dans l'une des urnes choisie au hasard. On demande de déterminer les répartitions rendant maximale la probabilité p de tirer une boule blanche.

Ici encore le résultat est tout à fait spectaculaire : le fait de mettre une seule boule blanche dans une première urne et toutes les autres (les blanches restantes et toutes les noires) dans la seconde, c'est-à-dire de prendre $r = s = 1$, rend p maximale ; il peut y avoir d'autres répartitions donnant le même p mais celle-là convient.

Nous ne donnerons pas le détail de la démonstration ; signalons simplement que l'on peut prouver cet optimum en calculant p à partir de b, n, r et s , puis en choisissant r en fonction de s supposé temporairement fixé de façon à maximiser p (c'était d'ailleurs la voie suggérée par l'énoncé distribué aux candidats). Ce qui est intéressant, c'est qu'un calcul de dérivée est ici inopérant, les variables prenant des valeurs entières et non continues.

Des généralisations portant sur le nombre de couleurs et le nombre d'urnes offertes au choix étaient également demandées. Saurez vous les mener à bien ? Si c'est le cas, vous avez peut-être vos chances dans un cabinet de recherche opérationnelle...

Le problème de Pearson (1857-1936)

Comment prendre une décision à partir d'observations statistiques ?

Nous ne pouvons malheureusement qu'effleurer l'immense domaine de la statistique mathématique, qui mérite un volume complet et n'est pas encore suffisamment médiatisé, et de ses liens complexes avec le calcul des probabilités, deux écoles au moins s'affrontant selon lesquelles on ne peut pas faire de statistiques sans avoir au départ quelques notions de probabilités, ou la proposition inverse. Leurs dates de naissance respectives sont 1654 pour les probabilités (correspondance Fermat-Pascal, relayée par *De ratiociniis in alea ludo* de Huygens vers 1657, *Ars conjectandi* de Jacques Bernoulli en 1713), et 1662 pour la statistique, d'abord uniquement descriptive (*Natural and Political Observations Mentioned in a Following Index, and Made upon the Bills of Mortality* de John Graunt, 1620-1674, et surtout deux textes de 1692 d'Edmund Halley *An Estimate of the Degrees of the Mortality of Mankind, Drawn from Curious Tables of the Births and Funerals at the City of Breslaw ; with an Attempt to Ascertain the Prices of Annuities upon Lives* et *Some Further Considerations on the Breslaw Bills of Mortality* d'après des documents prussiens adressés par Leibniz à la Royal Society).

Karl Pearson, ainsi que Student — en fait William Gosset (1876-1937), obligé de prendre un pseudonyme par les brasseries Guinness qui l'employaient comme

ingénieur — et le généticien Ronald Aylmer Fisher (1890-1962), ont travaillé à définir des tests mesurant la représentativité d'échantillons d'une population trop vaste pour pouvoir être étudiée de façon exhaustive. En particulier le test du χ^2 (prononcer : khi-deux) à ν paramètres de Pearson, adossé à la loi de probabilité de même nom appartenant à la famille des lois dites *Gamma*, a été introduit en 1900 par Pearson. Il a été enrichi en 1922 par son ancien assistant Udny Yule (1871-1951) et deux ans plus tard par Fisher. À l'instar de bien d'autres tests, il est d'usage constant, par exemple dans les hôpitaux universitaires, les usines mécaniques ou chimiques, les sociétés d'études politiques...

Pour donner un exemple très simple, utilisé dans la théorie des sondages bien connus à cause de leur répercussions dans les médias, citons juste une règle pour estimer la proportion p de personnes ayant une opinion donnée — par exemple contre la peine de mort — dans une population trop vaste pour pouvoir être interrogée de façon exhaustive : on constitue un échantillon de n personnes parmi lesquelles on trouve une fréquence f de sondés déclarant partager cette opinion. Il est normal de poser comme hypothèse que p est peu différent de f ; plus précisément, on peut montrer que dans des conditions optimales où p n'est pas trop proche de 0 ou de 1 et np reste compris entre 15 et $n - 15$, la valeur absolue de la différence entre p inconnue et f mesurée est inférieure ou égale à $\frac{1}{\sqrt{n}}$ avec 95% de certitude, c'est-à-dire une probabilité d'erreur inférieure ou égale à 5% (c'est la probabilité pour qu'une variable aléatoire normale s'écarte de sa valeur moyenne de plus de deux écart-types). Cette probabilité passerait à 2,6‰ si l'on demandait seulement l'inégalité plus lâche $\Pr(|p - f|) \leq \frac{3}{2\sqrt{n}}$ et au contraire à presque un tiers (trente-deux pour cent) pour

l'inégalité plus contraignante $\Pr(|p - f|) \leq \frac{1}{2\sqrt{n}}$. Par exemple, pour être convaincu avec un risque d'erreur de 5% que la majorité d'un pays a basculé vers l'abolition de la peine de mort en utilisant un échantillon de 1000 personnes, il faut que le nombre observé de ses adversaires soit au moins égal à 532 ($= \frac{n}{2} + \sqrt{n}$). Sous les conditions seuil à 0,05 et $n = 1000$, pour pouvoir affirmer qu'une proportion dépasse 50%, il faut observer une fréquence d'au moins 53,2% ; au seuil 0,001 il en faudrait au moins 55,3%. Cela éclaire d'un jour assez cru ce que signifient les « fourchettes » lorsque deux adversaires sont à 49 et 51% dans les sondages !

Un test est souvent utilisé lorsqu'il faut choisir entre deux hypothèses de travail dont l'une et l'une seulement est vraie, on est obligé de prendre deux risques en sens inverse : celui de rejeter la première hypothèse, souvent appelée *hypothèse nulle*, alors

qu'elle est vraie, erreur dite de première espèce dont la probabilité est traditionnellement notée α , et celui de rejeter la seconde, souvent appelée *hypothèse alternative*, alors qu'elle est vraie, erreur dite de deuxième espèce dont la probabilité est traditionnellement notée β . Le premier de ces nombres n'est calculable que si l'hypothèse nulle est suffisamment précise ; si l'on choisit pour hypothèse alternative la simple négation de l'hypothèse nulle — ce que nous ferons ci-dessous par commodité — il est rare que β soit alors calculable puisque l'on ne dispose généralement plus de description suffisamment complète de l'état de la population à sonder. Le nombre $1 - \beta$ est la probabilité de choisir l'hypothèse alternative lorsqu'elle est vraie : on l'appelle souvent la *puissance* du test. Il mesure sa capacité à ne pas faire rejeter à tort l'hypothèse nulle.

Cette dernière est notée H_0 ; elle doit paraître suffisamment vraisemblable, n'avoir jamais été contredite par l'expérience, satisfaire à un principe de prudence — par exemple en matière d'innocuité de médicaments nouveaux — et être simple dans son expression numérique. Nous allons borner cette présentation de la statistique inférentielle à une brève description du test du χ^2 , qui est en quelque sorte une extension de la technique précédente d'estimation d'une proportion par une fréquence.

Soit donc une certaine distribution représentée par $\nu + 1$ variables ; par exemple, toujours à propos d'un sondage, on aura $\nu = 3$ si l'on classifie des quidams en quatre catégories : très favorables, favorables, défavorables et très défavorables. Une certaine hypothèse H_0 étant posée, selon laquelle les valeurs estimées ou attendues (*expected* en anglais) ont été calculées à l'avance et notées E_i — par exemple H_0 peut signifier que l'on pense que les opinions n'ont pas varié depuis un recensement récent —, un échantillon est ensuite interrogé, qui donne des valeurs observées O_i *a priori* distinctes des E_i . On calcule alors :

$$\chi^2 = \sum_{i=1}^{\nu+1} \frac{(O_i - E_i)^2}{E_i}.$$

Une table dit que, pour $\nu = 3$, la probabilité pour que $\chi^2 \geq 7,815$ est de 0,05 si l'hypothèse posée H_0 est vraie ; on dit qu'elle est alors acceptable au seuil de signification 0,05 (ou plus exactement que l'on ne peut refuser H_0 à ce seuil puisque l'on admet que l'on a au moins 95% de chances de ne pas se tromper en l'acceptant si elle est vraie). Ce serait 0,1 pour $\chi^2 \geq 6,251$, événement moins difficile à réaliser. Il est en effet raisonnable de penser que plus le χ^2 est grand, plus les écarts entre les O_i et les E_i sont grands, et moins l'hypothèse nulle apparaît vraisemblable ; on pourra consulter par exemple *Le Jeu de la science et du hasard* de Daniel Schwartz, paru en 1994 chez Flammarion. Si l'on trouve $\chi^2 = 7$, c'est que l'hypothèse H_0 est vérifiée avec un

pourcentage compris entre 90 et 95% de chances de ne pas se tromper en affirmant que H_0 est vraie. L'opinion n'a donc sans doute pas varié de manière significative.

Le seuil $\alpha = 0,05$ est donc la probabilité de rejeter H_0 alors qu'en fait elle est vraie ; diminuer α conduit à ne plus pouvoir décider de la rejeter. Dans notre exemple, on dira que l'on refuse l'hypothèse au seuil de signification 0,1 mais qu'on l'accepterait au seuil 0,05 (*a fortiori* 0,01 et ainsi de suite) car l'expérience ne fournit alors aucun élément décisif contre H_0 .

La bizarrerie apparente consistant à prendre $\nu = 3$ alors qu'il y a quatre catégories s'explique parce que le nombre de *degrés de liberté* sur les E_i et les O_i doit être diminué de un puisque les sommes $\sum E_i$ et $\sum O_i$ sont naturellement égales à la taille de l'échantillon : en connaître trois détermine donc la dernière.

D'où vient le test du χ^2 ?

Comme souvent en statistique, la formule donnant le χ^2 semble très arbitraire. Nous pouvons donner ici une idée de son origine, à condition de connaître la notion de *loi binomiale* (enseignée au lycée) et d'avoir une intuition de ce qu'est la propriété connue sous le nom de *théorème de la limite centrée*, dont on pourra trouver une présentation dans de nombreux livres relativement élémentaires de calcul des probabilités.

Nous nous limiterons ici à $\nu = 3$ et à quatre classes, la méthode étant générale. Pour chaque indice i entre 1 et 4, le nombre d'occurrences O_i de personnes sondées appartenant à la classe i suit une loi binomiale $\mathcal{B}(n, p_i)$ où n est la taille de l'échantillon et p_i la proportion des individus formant la classe i . D'après les propriétés de la loi binomiale, l'espérance mathématique de O_i est $E(O_i) = E_i = np_i$, son écart-type est $\sigma_i = \sqrt{np_i(1-p_i)}$ que l'on peut grossièrement simplifier en $\sqrt{np_i} = \sqrt{E_i}$ puisque le carré d'un nombre entre 0 et 1 est, en toute première approximation, négligeable devant lui.

Au nombre d'occurrences O_i venant de la classe i , qui définit une variable aléatoire de type binomial, nous pouvons associer sa *variable aléatoire centrée réduite* X_i définie par l'égalité $X_i = \frac{O_i - E(O_i)}{\sigma_i} = \frac{O_i - E_i}{\sqrt{E_i}}$ d'après la simplification annoncée plus haut. Le théorème de la limite centrée nous dit que, si n est grand et p_i ni trop près de 0 ni de 1, X_i suit approximativement une *loi normale centrée réduite*, également connue sous le nom de loi de Laplace-Gauss d'espérance 0 et d'écart-type 1. D'autre part, on peut estimer que, si l'échantillon est tiré dans des conditions appropriées, trois parmi les quatre variables X_i ainsi définies sont indépendantes, la quatrième leur étant liée par l'égalité $\sum \sqrt{E_i} X_i = 0$, simple traduction de la relation évidente $\sum O_i - \sum E_i = n - n = 0$.

Un autre théorème de type limite centrée dit que, dans ces conditions, la variable aléatoire Q définie par l'égalité $Q = \sum_{i=1}^4 X_i^2$ suit une loi de probabilité dite du χ^2 à trois degrés de liberté, dont la densité est la fonction définie pour $t \geq 0$ par $\frac{1}{\sqrt{2\pi}} \sqrt{t} e^{-t/2}$ (il existe des formules analogues pour toute valeur entière de ν). En revenant aux définitions, on voit que l'on a exactement :

$$Q = \sum_{i=1}^4 \frac{(O_i - E_i)^2}{E_i} = \chi^2.$$

Si l'on regarde ce qui se passe pour $\nu = 1$, le test du χ^2 explique notre remarque de départ sur l'estimation d'une proportion p à partir d'une fréquence observée f . En effet, il y a ici dans la population de taille N deux classes, d'effectifs respectifs Np et $N(1-p)$; les effectifs correspondants attendus de l'échantillon de taille n sont donc $E_1 = np$ et $E_2 = n(1-p)$, alors que ceux qui sont réellement observés sont $O_1 = nf$ et $O_2 = n(1-f)$. Le χ^2 correspondant est, après calcul immédiat, égal à $\frac{n}{p(1-p)}(p-f)^2$. L'ennui vient ici du fait que $p(1-p)$ est inconnu; on pourrait le remplacer par $f(1-f)$, mais on peut aussi lui substituer son maximum $1/4$, puisque cette valeur est exacte pour $p = 1/2$ et reste proche de la réalité dans un large intervalle centré en $1/2$ (ainsi, $p(1-p) - (1/4) = -0,04$ pour $p = 0,3$). Par suite, $4n(p-f)^2$ est une assez bonne approximation du χ^2 dans ce cas. Une table donne d'ailleurs pour $\nu = 1$ que la probabilité d'avoir $\chi^2 \geq 4$ est égale à $0,05$ ce qui correspond au fait que la probabilité d'avoir $|p-f| \geq \frac{1}{\sqrt{n}}$ est bien égale à $1-0,95=0,05$. On trouverait de même $1-0,68=0,32$ pour $\chi^2 \geq 1$, qui correspond à $|p-f| \geq \frac{1}{2\sqrt{n}}$. Une table du χ^2 à un paramètre se déduit donc aussitôt de celle qui donne la célèbre fonction de répartition de la loi centrée réduite de Laplace-Gauss $\varphi(u) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^u e^{-x^2/2} dx$, ce qu'il est facile de vérifier dans les ouvrages spécialisés. De manière précise, pour $\nu = 1$ la probabilité pour que $\chi^2 \geq q \geq 0$ est égale à $2 \left(1 - \varphi(\sqrt{q})\right)$ puisque la densité du χ^2 est alors $\gamma(1/2, 2, t) = \frac{1}{\sqrt{2\pi}} \frac{e^{-t/2}}{\sqrt{t}}$ comme on le voit en posant $t = x^2$.

Le problème de Platon (428-348)

Les mathématiques existeraient-elles sans l'homme ?

Un débat philosophique immense, juste noté pour le plaisir, qu'on ne tranchera évidemment pas ici. Mais aussi, par raccroc, l'occasion de citer pêle-mêle les cinq solides réguliers, le concept de nombres irrationnels dont quelques racines carrées, et triplets pythagoriciens déjà cités : ces trois problèmes, tous liés à Platon, auront, surtout les deux derniers, une influence immense sur l'histoire des mathématiques.

Comme beaucoup de mathématiciens, même athées, Paul Erdős croyait en l'existence d'un « livre de Dieu » contenant toutes les démonstrations mathématiques possibles, connues et à venir, et surtout les meilleures. Espérons qu'il passe au moins une partie de son éternité à le déchiffrer et à marmonner parfois : « Bon sang, mais c'est bien sûr ! » Peut-être y a-t-il déjà lu la réponse à une question que l'un des auteurs de ce livre lui avait posée en 1972, pour laquelle il n'avait pu que regretter qu'il faille attendre l'an 2000 pour pouvoir espérer attaquer ce genre de conjectures. Au fait, 2000 a fini par arriver ; il faudrait peut-être retrouver ce vieux dossier poussiéreux...

Paul Erdős, l'homme pressé

Né à Budapest le 26 mars 1913, Pál Erdős est mort à Varsovie le 20 septembre 1996, après avoir passé sa vie à se promener inlassablement dans le monde entier, passant d'un avion à l'autre avec ses deux petites valises contenant presque tout son bagage. L'un de ses biographes le décrira comme l'un de ces colporteurs que l'on voyait, vers la fin du XIX^e siècle, apporter dans leur boîte de bois toutes les nouveautés pour allécher le chaland. Cet homme était aussi pressé que bizarre : adonné aux amphétamines de toutes sortes, auteur de la définition d'un mathématicien comme simple machine à transformer le café en théorèmes, se lavant les mains cinquante fois par jour, il ne portait que des vêtements de soie pour éviter des allergies, travaillant parfois dix-neuf heures par jour pendant lesquelles il écrivait au moins cinq lettres ou cartes postales dans le monde entier ! Il fut également extraordinaire à bien d'autres points de vue. Il a par exemple publié quelque 1475 articles, avec entre 450 et 500 coauteurs (titulaires du nombre d'Erdős égal à n , toute personne ayant écrit un article en commun avec quelqu'un dont le nombre d'Erdős est égal à n se voyant créditée d'un nombre égal à $n + 1$ si elle n'en possédait pas déjà un autre plus petit auparavant).

Docteur à dix-neuf ans, il avait trouvé dès sa dix-huitième année une nouvelle démonstration élémentaire du postulat de Bertrand démontré par Tchebitcheff (il existe au moins un nombre premier dans tout intervalle du type $[n, 2n]$). Il était connu comme un excellent chercheur, trouvant des solutions originales dans différents domaines comme la théorie des nombres, la théorie des graphes, la combinatoire, les développements asymptotiques de fonctions arithmétiques, et surtout réputé pour son exceptionnelle aptitude à poser des problèmes et des

conjectures puis à les résoudre avec le mathématicien le plus apte qu'il avait lui-même sélectionné à cette fin.

Cette homme à la collaboration si féconde connaîtra pourtant un échec dans une relation humaine d'autant plus importante pour lui qu'elle concerne son plus grand succès : avoir contribué de façon décisive à l'élaboration d'une démonstration élémentaire du théorème de Hadamard et La Vallée-Poussin. En 1949, il est mis au courant par Paul Turàn (1910-1976) d'une inégalité due à Atle Selberg, Norvégien travaillant aux États-Unis, que ce dernier avait développée comme une étape possible vers une telle démonstration élémentaire, mais présentée à Erdős comme insuffisamment puissante. En quelques heures, ce dernier dément le pessimisme de Selberg, fait une avancée décisive à partir de laquelle Selberg n'a aucun mal à boucler la preuve. Un papier joint de plus aurait été l'exacte reconnaissance des apports de chacun, de valeur sans doute égale. Malheureusement les cartes postales envoyées dans l'enthousiasme par l'imprudent Erdős peuvent laisser penser que le mérite essentiel lui revient : Selberg se bloque, refuse toute collaboration nouvelle, trouve un passage détourné pour publier un article ne devant formellement plus rien à son rival. Il recevra, seul, la médaille Fields en 1950, Erdős — qui de son côté avait lui aussi découvert comment contourner les découvertes de Selberg — devant se contenter du prix Wolf en 1984. Sur les 50 000 dollars qui lui seront donnés à cette occasion, il en retiendra 720 pour son usage privé, léguant le reste à différentes institutions, dont le Technion à Haïfa, où il était professeur invité permanent, pour la création d'une chaire portant le nom de ses parents, nés Anna Wilhelm et Lajos Engländer, tous deux professeurs de lycée dans un pays où cette profession est considérée comme aussi noble que celle de médecin ou d'avocat. Les deux sœurs de Pål, Klåra et Magda, respectivement âgées de trois et cinq ans, avaient été emportées par une épidémie de scarlatine pendant que leur mère accouchait de leur frère : une telle tragédie n'explique nullement son génie, mais peut éclairer certaines de ses bizarreries.

Erdős resta incroyablement fécond toute sa vie solitaire. En Hongrie, où il est vénéré, il restera comme une exception pour au moins une particularité qu'il fut le seul à connaître : le régime communiste lui avait offert un « passeport spécial », lui permettant, même après la répression de 1956, de voyager à sa guise. Deux livres lui ont été consacrés : *My Brain Is Open*, par Bruce Schechter chez Simon & Schuster et *The Man Who Loved Only Numbers*, par Paul Hoffmann chez Hyperion, tous deux en 1998 (le dernier a été traduit en français par Maurice Mashaal chez Belfin). Ils rendent bien compte tous deux de l'extraordinaire parcours de l'auteur du concept de « Livre de Dieu », où plutôt du « Livre du Fasciste suprême » selon sa terminologie elle aussi tout à fait particulière...

Le problème de Poincaré (1854-1912)

La deuxième conjecture la plus « résistante » à ce jour.

Nous voici dans le grand chantier de la topologie, longtemps connue sous le nom d'*Analysis situs*, qui fut le domaine de recherches actives conduites de Leonhard Euler à Pavel Alexandrov (1896-1982) et Stephen Smale (1930-2000), connu du public en 1957 par le retournement de la sphère — par quatorze transformations sans la déchirer ni la plier —, qui a pu être vulgarisé avec succès, en passant par Luitzen Brouwer (1881-1966) et Henri Lebesgue (1875-1941).

Si les théorèmes fondamentaux sont bien établis aujourd'hui, comme ce qui touche à la dimension — concept purement algébrique au départ —, il reste quelques énigmes fortes non résolues, comme cette proposition d'Henri Poincaré sur des caractérisations des sphères de dimension n (la sphère usuelle est de dimension 2 parce que décrite par deux paramètres, et la sphère de dimension 1 est la circonférence). Elles paraissent bien vraisemblables, et furent certes démontrées, non sans difficultés, par Smale en 1960 pour $n \geq 5$ et Mike Freedman en 1983 pour $n = 4$, sauf... pour le cas $n = 3$. Revenons à l'énoncé de Poincaré en 1904, année de l'axiome du choix de Zermelo : toute variété compacte à trois dimensions dont le groupe fondamental est trivial (dont tout cercle peut être compacté en un point) est homéomorphe à la sphère. Celui qui comblera cette exception irritante, dans un sens ou dans l'autre, sera bien vite célèbre, mais il lui faudra une technique exceptionnelle, sans doute analogue à celle d'un Wiles. Il gagnera de plus 1 million de dollars, puisque ce problème a été repris par le Clay Institute dans sa séance du 24 mai 2000 au Collège de France à Paris.

Le problème de Riemann (1826-1866)

La première conjecture la plus « résistante » à ce jour.

Tout aussi redoutable que le précédent, sinon même davantage, celui-ci concerne les zéros non triviaux de la célèbre fonction ζ (prononcer : *dzéta*), découverte par Euler puis étendue à des valeurs complexes de la variable : ces racines auraient toutes $1/2$ comme partie réelle. Cette hypothèse joue un rôle essentiel dans de nombreuses parties de l'analyse, mais surtout dans la théorie des nombres premiers.

Son histoire remonte à une affirmation de Riemann en 1859, présentée sans aucune justification, mais qui possède des analogues en géométrie algébrique : André Weil (1906-1998) et Pierre Deligne (né en 1944) ont montré que ces conjectures sont exactes. Mais leurs travaux, très complexes, n'ont pas permis pour l'instant de confirmer l'intuition riemannienne, et *a fortiori* pas davantage ce qui est connu sous le

nom d'« hypothèse généralisée de Riemann », qui permettrait un grand progrès pour certaines formules en théorie des nombres.

Ce problème est le seul à être commun aux listes de Hilbert en 1900 et du Clay Institute en 2000.

Citons une curiosité. Il existe au moins un théorème qui a été démontré en deux temps : si l'hypothèse de Riemann est vraie, alors... ; si elle ne l'est pas, alors... Cela s'appelle assurance tous risques et principe de précaution !

Le problème de Turing (1912-1954)

Ce programme aura-t-il une fin ?

Il n'y a pas d'algorithme pour dire à coup sûr si un algorithme donné traduit par un programme informatique fournira un résultat au bout d'un certain temps ou s'il bouclera sans fin. Et c'est subtil, mais (presque) facile à comprendre, comme on le verra dans le chapitre « Mathématiques et information (2) ».

Le problème de Zénon (V^e siècle av. J.-C.)

Qu'est-ce que la somme d'une série ?

L'infini chez les Grecs : un Eudoxe commencera à entrevoir, au siècle suivant, comment le concept d'approximation introduit discrètement celui de limite. Chez Zénon, auteur de quatre paradoxes très connus, il est brutalement sous-jacent, quoique de manière évidemment indirecte. En expliquant qu'Achille ne peut pas rattraper la tortue puisqu'il lui faut d'abord arriver à son point de départ, puis atteindre, une à une, une infinité de positions qu'elle quitte tour à tour avant qu'il ne la rejoigne, il affirme implicitement qu'une somme infinie de longueurs (ou d'intervalles de temps) ne peut avoir de sens fini.

Tout cela a été clarifié avec le calcul des séries, dont la théorie a occupé de grands esprits comme Newton, Gauss et Karl Weierstrass (1815-1897). Et pourtant tout n'est peut-être pas encore tout à fait limpide, des mathématiciens philosophes pensant toujours que l'infini *potentiel* ne règle pas toutes les difficultés. La réponse classique à la question : « Que signifie l'expression $\sum_{o}^{+\infty} 2^{-n} = 2 ?$ » est qu'il s'agit

simplement d'une écriture abrégée pour dire que, pour approcher 2 de moins de ε , il suffit d'ajouter entre eux les termes d'un paquet, fini mais peut-être très grand,

extrait de la somme. Pour certains, il est au contraire toujours essentiel d'accepter l'idée d'un infini *actuel* — une somme infinie ayant un sens pour elle-même, pas seulement comme valeur chimérique —, un peu comme l'analyse dite *non standard* de 1960 d'Abraham Robinson (1918-1974) a réhabilité les nombres infiniment grands et petits. D'autres réponses aussi étranges viendront peut-être modifier notre vision des arguties de Zénon d'Élée, heureusement sans mettre en péril les constructions des ingénieurs et architectes bâties grâce aux formules habituelles donnant la somme d'une série géométrique !

Le problème de Zermelo (1871-1953)

L'axiome du choix est-il acceptable ?

Étant donnée une famille d'ensembles $(E_i)_{i \in I}$, il existe au moins une application qui, à tout indice $i \in I$, associe un élément de E_i (1904).

Un axiome difficile de la théorie des ensembles, plus ou moins évident selon la forme qu'on lui donne, nécessairement déroutant, surpuissant, dont on ne peut pas se passer en théorie — une très large partie de l'analyse, voire de l'algèbre, reposant sur son utilisation parfois bien cachée —, objet de discussions farouches au début du XX^e siècle, mais dont (presque) tout le monde se moque aujourd'hui dans la pratique des mathématiques courantes puisque tout le monde l'accepte au nom du principe de « commodité » cher à Henri Poincaré.

Il n'en va pas de même pour le problème de Cantor, auquel on le compare parfois en raison des théorèmes de Gödel et de Cohen qui les concernent tous les deux ; il est vrai que les interventions des hypothèses sur le continu ont un rôle bien moindre dans la vie quotidienne du mathématicien de base que celles qui ont bouleversé Baire, Borel, Hadamard et Lebesgue.

À quoi sert la logique ? Pour l'instant, peut-être plus à grand-chose (sauf à nourrir les logiciens, suivant une vieille blague), mais qui peut prédire qu'il n'y aura pas demain ou après-demain une nouvelle crise des « fondements » qui nous obligera à mieux balayer devant notre porte ? Malheur à qui oserait dire que les mathématiques ont terminé leur Big Bang !

Des problèmes par centaines

Une précision ici s'impose : le choix de ces quarante grands problèmes nous a été dicté par le souci de couvrir aussi largement que possible l'immense champ des mathématiques. Le nombre des autres problèmes — restés célèbres à quelque titre — à s'être posés aux mathématiciens en différentes occasions est évidemment beaucoup plus élevé, justifiable de considérations historiques ou scientifiques. Citons-en au hasard, au plaisir des réminiscences d'heures riches en joies diverses.

C'est par exemple le problème de Didon, lorsqu'après le meurtre de son mari, la reine de Tyr venue se réfugier en Afrique, là où devait naître Carthage, reçut en propriété du roi Yarbass, nous affirme Virgile, « tout le territoire qu'elle pourrait englober avec une peau de bouc ». Elle la découpa en fines lamelles qu'elle mit bout à bout de manière à en faire un périmètre auquel elle conféra une forme circulaire : un calcul virtuel, sorte de recherche opérationnelle avant la lettre, l'avait convaincue qu'à périmètre égal, un cercle offre la plus grande surface. Ce problème est devenu un classique des mathématiques, étendu à trois dimensions avec la recherche des surfaces minimales délimitant un volume donné : s'il s'agit d'une surface fermée c'est la sphère, et c'est une caténoïde (surface engendrée par la révolution d'une chaînette) si elle doit s'appuyer sur des cercles. Une grande surprise de la géométrie moderne a été de découvrir l'étrangeté des solutions qui s'offrent dans un espace de dimension n , n étant cette fois-ci strictement supérieur à trois.

C'est le problème du joueur d'échecs auquel on demande une opération telle que le passage du cavalier de la case p à la case q — ce problème ayant été longuement étudié au début du XVI^e siècle par Guarini di Forti —, ou un algorithme de victoire si elle est possible.

Le jeu du fer à cheval

Une étude mathématique exhaustive a démystifié le jeu du fer à cheval, très répandu autrefois en Europe, singulièrement dans le Jura et en Alsace.

Cinq emplacements, le centre d'un X et ses extrémités, peuvent être occupés par des pions que l'on déplace d'une case, sachant que la position centrale, dite 0 permet d'atteindre toutes les autres. Le passage de 1 à 4 est interdit, d'où un organigramme de fer à cheval : ainsi, depuis 1, on ne peut gagner que 0 ou 2 et depuis 4 on ne peut gagner que 0 ou 3. Les cases 2 et 3 laissent chacune trois possibilités, respectivement 1, 0, 3 et 2, 0, 4.

La partie se dispute à deux, A possède deux pions blancs et B deux pions noirs. Ils jouent à tour de rôle, chacun déplaçant l'un de ses pions d'une case à son gré. Le perdant est celui qui se trouve bloqué.

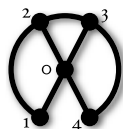


figure 35. Le jeu du fer à cheval

Au début, *A* choisit 2 cases à sa guise et *B* met ses pions sur 2 des trois cases restantes. Si l'on tient compte des symétries, cela fait apparaître 16 conditions initiales possibles, autrement dit on se trouve en présence de 16 jeux différents justifiables d'algorithmes avec ces issues :

- *A* est gagnant s'il choisit 1, 2 ou 1, 5 et *B* opte pour 3, 4.
- *B* est gagnant s'il choisit 0, 3 sur 1, 2 de *A*.
- dans les treize autres cas, la partie sera nulle.

Ce sont les carrés magiques pandiagonaux « plus que parfaits » généralisant les carrés de Dürer, faits de n^2 cases contenant les entiers de 0 à $n^2 - 1$ avec la contrainte d'un total identique sur toutes les lignes, toutes les colonnes et les diagonales : les diagonales principales et les $2n - 2$ autres « brisées », c'est-à-dire formées de deux sous-diagonales chacune parallèle à une diagonale principale, correspondant à des rangées disjointes ce qui permet de les réunir en une seule diagonale virtuelle. Il faut de plus que les sommes des quatre nombres formant un carré défini par deux lignes contiguës et deux colonnes contiguës soient toutes égales (ainsi qu'une autre propriété analogue ; voir par exemple le très documenté *Les Carrés magiques*, de René Descombes, page 159, Vuibert 1999). Pour $n = 3$ et $n = 4$, la solution est connue depuis (au moins) trois siècles. Quand n croît, les difficultés augmentent. De nombreuses études ont été consacrées à ce type de problème. Nous donnons ci-après une « super-solution » pour $n = 8$ de Kathleen Ollerendhaw et David Brée qui a récemment défrayé la chronique. On y constatera que chacune des sommes usuelles dans la théorie des carrés parfaits y est égale à 252, y compris pour les huit diagonales, mais que les sommes des quatre nombres en carrés sont toutes égales à 126. Enfin sur chaque diagonale, principale ou brisée, deux cases séparées par trois ($= (8/2) - 1$) cases ont une somme constante, égale à 63. Bien entendu, les deux auteurs ont trouvé une méthode générale pour construire des carrés *hypermagiques* comme celui-là. Il est tout à fait remarquable que Dame Kathleen Ollerendhaw ait été âgée de quatre-vingt-cinq ans lorsqu'elle a résolu ce problème de combinatoire très difficile, il est vrai après quarante ans de conjectures et d'efforts incessants...

Ce sont les problèmes de métalangage lorsqu'on vous demande de dire quelque chose sachant qui si c'est une vérité vous serez fusillé, tandis que si c'est une erreur

0	62	2	60	11	53	9	55
15	49	13	51	4	58	6	56
16	46	18	44	27	37	25	39
31	33	29	35	20	42	22	40
52	10	54	8	63	1	61	3
59	5	57	7	48	14	50	12
36	26	38	24	47	17	45	19
43	21	41	23	32	30	34	28

figure 36. Le carré super-magique de Ollerendhaw et Brée

vous serez pendu. La solution est pour vous de prononcer la phrase : « Je serai pendu ». Citons aussi la feuille de papier ne quittant pas le bureau de l'un d'entre nous, où il est écrit au recto « ce qui est écrit au dos de ce papier est vrai » et, au verso, « ce qui est écrit au dos de ce papier est faux ».

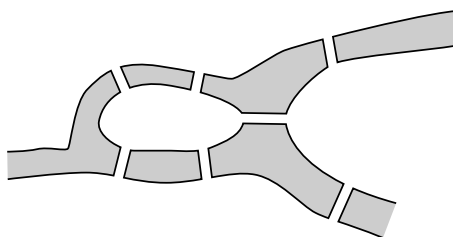


figure 37. Le célèbre problème des 7 ponts de Königsberg

C'est l'histoire des sept ponts sur la Pregel de Königsberg, une cité dans laquelle un promeneur (Kant ?) pouvait se demander si un jour il trouverait un itinéraire lui permettant de passer par ces sept ponts, une et une seule fois pour chacun. Euler devait indiquer une méthode, annonciatrice de la topologie, à savoir la représentation de l'ensemble des points par un graphe assorti d'un théorème prenant en considération le *degré* d'un sommet, mesuré par le nombre des arcs qui en émanent. Aujourd'hui, nous sommes donc en mesure de dire immédiatement que, le graphe de Königsberg comportant quatre sommets de degré impair, le problème posé n'avait pas de solution.

