

Marcus du Sautoy

Le mystère des nombres

folio essais



COLLECTION
FOLIO ESSAIS

Marcus du Sautoy

Le mystère des nombres

Odyssée mathématique
à travers notre quotidien

*Traduit de l'anglais
par Hélène Borraz*

Gallimard

Né en 1965, Marcus du Sautoy est professeur de mathématiques à l'université d'Oxford et spécialiste de la théorie des groupes. Intervenant au Collège de France et à l'École normale supérieure, il se consacre également à la popularisation des mathématiques en les présentant de manière aussi limpide que ludique.

Pour Shani

Introduction

Le changement climatique est-il une réalité ? Notre système solaire peut-il soudain voler en éclats ? Est-il risqué de communiquer son numéro de carte bancaire sur Internet ? Comment pouvons-nous faire pour gagner contre le casino ?

Depuis que l'homme est capable de communiquer, il se pose des questions et tente de prédire l'avenir en s'efforçant de comprendre le monde autour de lui. L'outil le plus puissant créé par l'homme pour l'aider à naviguer dans la complexité de ce monde, ce sont les mathématiques.

De la trajectoire d'un ballon de foot au suivi démographique des lemmings, du déchiffrement de codes à la stratégie gagnante au Monopoly, les mathématiques offrent les clés pour comprendre les mystères de la nature. Mais les mathématiciens n'ont pas réponse à tout. Il existe de nombreuses questions fondamentales dont nous débattons encore.

Dans chacun des chapitres de ce livre, je vous invite à découvrir non seulement un grand thème des mathématiques mais aussi une énigme non élucidée parmi les plus célèbres problèmes non résolus de tous les temps.

Sachez que si vous trouvez la solution à certains de ces casse-tête, vous serez non seulement célèbre, mais aussi riche. En effet, un homme d'affaires américain, Landon Clay, promet de donner un million de dollars à quiconque résoudra l'un de ces mystères mathématiques. Si Landon Clay est prêt à donner autant d'argent pour une formule mathématique, c'est parce qu'il a parfaitement compris que l'ensemble des sciences, des technologies, des phénomènes économiques et même l'avenir de notre planète ont pour fondements les mathématiques. Soyez donc attentif, à la fin de chaque chapitre, à la présentation du casse-tête : un million de dollars sont à la clé !

Le premier chapitre, « Le curieux incident des interminables nombres premiers », a pour thème l'objet de base de l'arithmétique, les nombres. Je vous ferai découvrir les nombres premiers : les plus

importants mais aussi les plus énigmatiques des nombres du monde mathématique. Ils détiennent un secret qui pourrait vous rapporter gros.

Dans le chapitre II, « L'étrange affaire de la forme insaisissable », nous partirons à la découverte des formes étranges et merveilleuses qui nous entourent — le dé, la bulle, le sachet de thé, le flocon de neige... — avant de nous attaquer au plus grand des défis : connaître la forme de notre univers.

Grâce au chapitre III, « Le secret des coups gagnants », nous verrons comment tirer profit de la logique mathématique et des probabilités dans le contexte des jeux d'argent. Que vous jouiez avec des billets de Monopoly ou des espèces sonnantes et trébuchantes, les mathématiques peuvent vous mettre sur la voie de la victoire. Il existe cependant des jeux simples que même les plus grands esprits peinent à résoudre.

La cryptographie sera le sujet du chapitre IV intitulé « Le cas du code incassable ». Les mathématiques apportent souvent la clé pour déchiffrer un message secret. Mais je vais vous révéler comment les mathématiques permettent de créer de nouveaux codes afin de communiquer en toute sécurité sur Internet, d'envoyer des messages dans l'espace et même de lire dans les pensées de vos amis.

Le chapitre V est consacré à un rêve que nous avons tous, celui de prédire l'avenir. Je vous expliquerai comment certaines équations mathématiques sont en réalité d'excellentes diseuses de bonne aventure. Elles permettent d'anticiper les éclipses, d'expliquer pourquoi un boomerang revient et même de prédire l'avenir de notre planète. Certaines de ces équations demeurent pourtant encore non résolues. Pour conclure ce dernier chapitre, nous aborderons la question fascinante de la turbulence, laquelle affecte un nombre incalculable de choses, des coups francs de David Beckham aux avions dans le ciel, tout en restant un des grands mystères mathématiques.

Les principes mathématiques présentés dans cet ouvrage sont d'une difficulté variable. Les problèmes exposés en conclusion de chaque chapitre sont, en revanche, tellement difficiles que personne n'est encore parvenu à les résoudre. Lorsque nous lisons pour la première fois des auteurs tels que Shakespeare ou Steinbeck, nous découvrons à quel point la littérature est fascinante. De la même manière, lorsque nous entendons Mozart ou Miles Davis pour la première fois, la musique prend soudain vie. Mais jouer du Mozart est loin d'être facile, tout comme lire

Shakespeare peut représenter un vrai défi, même pour les lecteurs les plus avisés. Cela ne signifie pas que l'on doive réserver leurs œuvres aux seuls spécialistes. La même chose vaut pour les mathématiques. Si cela peut parfois vous sembler difficile, prenez simplement du plaisir à découvrir et rappelez-vous ce que vous aviez ressenti lors de votre première lecture de Shakespeare.

À l'école, nous apprenons que les mathématiques sont fondamentales. Pour vous en convaincre, je souhaite vous montrer à quel point elles sont vivantes et vous expliquer certaines des plus importantes découvertes mathématiques réalisées à ce jour. En vous proposant plusieurs problèmes non résolus, je veux aussi vous donner l'occasion de vous comparer aux plus grands cerveaux de l'Histoire. À l'issue de cet ouvrage, j'espère que vous comprendrez à quel point les mathématiques sont au cœur de notre quotidien.

À propos des sites Web

Tout au long du livre, je me réfère à des fichiers PDF que vous pouvez télécharger sur la page du site de mon éditeur anglais 4th Estate dédiée au présent ouvrage : <http://www.4thestate.co.uk/2012/08/numbermysteries/> afin de participer à certains jeux ou construire diverses formes mentionnées dans le texte.

Des liens vers d'autres sites sont également proposés au fil des pages. Il est possible d'y accéder en saisissant l'adresse dans votre moteur de recherche.

Il est également possible d'acquérir l'application Num8er My5teries appelée « Marcus du Sautoy's Number Mysteries », que vous téléchargerez sur votre iPhone pour accéder à diverses versions interactives de nombreux jeux mentionnés tout au long du livre.

Voici quelques sites Web supplémentaires (en langue anglaise) que nous vous conseillons de visiter :

www.conted.ox.ac.uk

www.rigb.org/christmaslectures06

<https://people.maths.ox.ac.uk/dusautoy>

www.simonyi.ox.ac.uk

<http://twitter.com/MarcusduSautoy>

www.mangahigh.com

www.whatevertrevor.com

www.claymath.org

www-groups.dcs.st-and.ac.uk/~history

<http://mathworld.wolfram.com>

<http://bit.ly/Mathemagicians>

Chapitre premier

LE CURIEUX INCIDENT DES INTERMINABLES NOMBRES PREMIERS

1, 2, 3, 4, 5... c'est si simple : ajoutez 1 et vous obtenez le nombre suivant. Mais avons-nous conscience que sans les nombres nous serions perdus ? Arsenal contre Manchester United — qui a gagné ? Mystère. Chaque équipe a pas mal marqué... Vous cherchez quelque chose dans l'index de cet ouvrage ? L'explication sur la manière de gagner au loto se trouve quelque part vers le milieu du livre. Et le loto lui-même ? Impossible sans les nombres. N'est-il pas extraordinaire de constater à quel point le langage des nombres est essentiel à notre relation au monde ?

Même chez les animaux, les nombres sont fondamentaux. Une meute décidera de fuir ou d'attaquer un groupe rival selon que le nombre des membres dépasse ou non celui des siens. L'instinct de survie des animaux repose en partie sur leur aptitude mathématique. Ainsi, derrière la simplicité apparente de la suite des nombres se cache un des plus grands mystères des mathématiques.

2, 3, 5, 7, 11, 13... Voici les nombres premiers, les nombres indivisibles qui constituent les blocs de construction de tous les autres nombres — les atomes du monde des mathématiques, véritables petits joyaux sertis dans l'infinie étendue des nombres.

En dépit de leur importance, les nombres premiers demeurent une des plus grandes énigmes rencontrées au cours de la quête de la connaissance. Comme il ne semble pas y avoir de formule magique permettant de passer d'un nombre premier au suivant, la question de leur détermination demeure un mystère comparable à un trésor enfoui dont personne ne connaîtrait la cachette.

Dans ce chapitre, nous regarderons ce que nous savons effectivement de ces nombres si particuliers. Ce faisant, nous

découvrirent que certaines civilisations anciennes ont tenté d'identifier et de réfléchir sur les nombres premiers et que les musiciens ont exploité le rythme syncopé de leur apparition. Nous apprendrons pourquoi les nombres premiers ont été utilisés pour communiquer avec des extraterrestres et comment ils nous permettent de conserver des choses secrètes sur Internet. En fin de chapitre, j'aurai le plaisir de proposer une énigme mathématique à base de nombres premiers qui, si vous parvenez à la résoudre, vous rapportera un million de dollars. Mais avant de s'attaquer à ce casse-tête majeur des mathématiques, commençons par aborder l'un des grands mystères numériques de notre temps.

POURQUOI BECKHAM A-T-IL CHOISI LE MAILLOT 23 ?

Lorsque David Beckham a rejoint le Real Madrid en 2003, il a choisi de jouer avec le maillot portant le numéro 23. Voilà un bien étrange choix, se disaient les supporters, car jusqu'alors, que ce soit dans l'équipe d'Angleterre ou à Manchester United, il jouait avec le numéro 7. Le problème, c'est que dans l'équipe madrilène le numéro 7 était déjà pris par Raúl, et il était hors de question pour l'Espagnol de renoncer à son maillot pour ce *glamour-boy* venu d'Angleterre.

Diverses théories furent avancées pour expliquer le choix de Beckham, la plus répandue étant celle liée à Michael Jordan. Le Real Madrid souhaitait conquérir le marché américain afin d'exploiter l'immense potentiel commercial que représenterait la vente du maillot de Beckham. Mais aux USA, le football n'est pas un jeu très populaire. Ce que les Américains aiment, c'est le basket et le base-ball, des sports dont les matchs se terminent sur des scores du style « 100 à 98 », avec forcément un vainqueur. Ils ne voient pas l'intérêt d'un sport pouvant, à l'issue de quatre-vingt-dix minutes de jeu, se terminer par un match nul.

Selon cette théorie donc, le Real Madrid mena une enquête et détermina que Michael Jordan, marqueur de paniers prolifique des Chicago Bulls, était de toute évidence le joueur de basket le plus célèbre du monde. Durant toute sa carrière, Jordan a porté le maillot numéro 23. Il suffisait donc pour le Real de mettre un 23 sur le dos d'un maillot de foot, de croiser les doigts et d'espérer que

l'association avec Jordan opère sa magie afin de pénétrer le marché américain.

Pour certains, cette hypothèse était trop cynique ; cependant ils en proposèrent une plus sinistre encore. Jules César fut assassiné de 23 coups de couteau dans le dos. Ce choix pour le propre dos de Beckham était-il un mauvais présage ? D'autres encore ont avancé que ce choix était peut-être lié à la fascination que Beckham voue à *La Guerre des étoiles* (la princesse Leia est emprisonnée dans le bloc de détention AA23 dans le premier film de la série). À moins que Beckham soit un adepte secret du discordianisme, un culte des années 1950 qui vénère le chaos et entretient une obsession cabalistique pour le nombre 23...

Mais dès que j'ai vu le numéro sur le maillot de Beckham, une solution plus mathématique m'est venue à l'esprit. 23 est un nombre premier. C'est-à-dire un nombre qui n'est divisible que par lui-même et par 1. 17 et 23 sont des nombres premiers car on ne peut pas les écrire en multipliant deux nombres plus petits, alors que 15 n'est pas un nombre premier car on peut écrire $15 = 3 \times 5$. Les nombres premiers sont les plus importants en mathématiques, en effet tous les nombres entiers sont construits en multipliant des nombres premiers entre eux.

Prenez 105, par exemple. Ce chiffre est clairement divisible par 5. Donc je peux écrire $105 = 5 \times 21$. 5 est un nombre premier, un nombre indivisible, mais ce n'est pas le cas de 21 : je peux l'écrire sous la forme de 3×7 . Ainsi, 105 peut s'écrire $3 \times 5 \times 7$. Mais je ne peux pas aller plus loin. Je peux faire cela avec n'importe quel nombre puisque chaque nombre est soit premier et indivisible, soit non premier et donc le produit de nombres indivisibles plus petits.

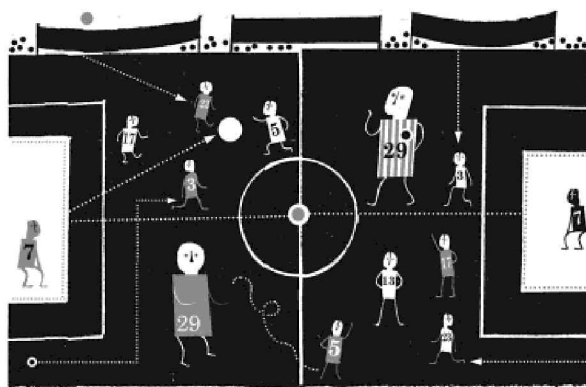


Fig. 1.01

Les nombres premiers sont les blocs de construction, les briques de tous les nombres. Tout comme les molécules sont construites à partir d'atomes tels que l'hydrogène et l'oxygène ou le sodium et le chlore, les nombres sont construits à partir de nombres premiers. En arithmétique, les nombres 2, 3 et 5 sont comme l'hydrogène, l'hélium et le lithium. C'est ce qui fait d'eux les nombres les plus importants des mathématiques. De toute évidence, ils revêtaient une très grande importance aussi aux yeux du Real Madrid.

UN MATCH DE RÊVE ENTRE NOMBRES PREMIERS

Téléchargez le fichier PDF de ce jeu sur la page Web dédiée au présent ouvrage. Chaque joueur découpe trois joueurs de type subbuteo et choisit différents nombres premiers qu'il inscrit sur leur dos. Utilisez un des ballons de Platon.

Le ballon est donné à un joueur de l'équipe 1. L'objectif est de franchir les trois joueurs de l'équipe adverse. L'adversaire choisit le premier joueur qui tentera de tacler le joueur de l'équipe 1. Lancez le dé. Le dé a six faces : 3, 5 et 7 blancs et 3, 5 et 7 noirs. Le dé vous indique si vous devez diviser par 3, 5 ou 7 le nombre premier de votre joueur et celui du joueur de l'équipe adverse, puis vous prenez le reste. Si le dé affiche un 3, 5 ou 7 blancs, le reste doit être égal ou supérieur au reste de l'adversaire. Si le dé affiche un 3, 5 ou 7 noirs, le reste doit être égal ou inférieur à celui de l'équipe adverse.

Pour marquer un but, vous devez avoir franchi un à un les trois joueurs et affronter un choix aléatoire de nombres premiers annoncé par l'équipe adverse. Si à un moment donné l'adversaire vous bat, alors c'est l'équipe adverse qui prend possession du ballon. La personne qui a remporté la possession du ballon utilise alors le joueur qui a gagné pour essayer à son tour de franchir les trois joueurs de l'équipe adverse. Si le tir de l'équipe 1 ne marque pas de but, alors l'équipe 2 prend le ballon et le donne à un de ses joueurs.

Le match sera remporté par l'équipe qui marque soit le plus de buts en un temps limité, soit les trois premiers buts.

Quand j'ai commencé à regarder d'un peu plus près l'équipe du Real, j'ai soupçonné la présence d'un mathématicien sur le banc. Après une petite enquête, j'ai pu constater qu'au moment de l'arrivée de Beckham à Madrid, tous les *galácticos*, les joueurs phares du Real, arboraient des maillots portant des nombres premiers : Carlos (pilier de la défense), le 3 ; Zidane (milieu offensif), le 5 ; Raúl et Ronaldo (principaux attaquants du Real), le 7 et le 11. Il était donc sans doute inévitable que Beckham se voie lui aussi attribuer un nombre premier, un numéro auquel il est désormais très attaché : lors de son transfert au LA Galaxy, il insista pour conserver son numéro dans sa tentative de convertir le public américain à l'art du foot.

Même si cela peut paraître irrationnel de la part d'un mathématicien, qui est censé penser de manière analytique et logique, j'ai moi aussi choisi de porter un nombre premier dans mon équipe de foot, le Recreativo Hackney. Notre équipe n'ayant pas tout à fait l'envergure du Real Madrid, j'ai choisi le 17, un

nombre premier plutôt sympa, comme nous le verrons plus tard. Mais lors de notre première saison, l'équipe n'a pas particulièrement brillé. Nous jouions dans la deuxième division du London Super Sunday League, et nous avons terminé tout en bas du tableau. Heureusement, comme il s'agit de la division la plus basse de Londres, il ne nous restait plus qu'à remonter.

Comment faire pour améliorer notre classement ? Peut-être le Real avait-il une piste — jouer avec des maillots portant des nombres premiers donnait-il un avantage psychologique ? Peut-être étions-nous trop nombreux dans l'équipe à jouer avec des maillots ne portant pas des nombres premiers, par exemple le 8, le 10 ou le 1. La saison suivante, j'ai convaincu l'équipe de changer de maillots, et nous avons tous joué avec des nombres premiers : 2, 3, 5, 7... jusqu'au 43. Nous étions métamorphosés. Pourtant, une fois arrivés en première division, nous nous sommes rapidement rendu compte que « l'effet nombre premier » ne dure que le temps d'une saison. À nouveau relégués en deuxième division, nous cherchons désormais une autre théorie mathématique capable de nous donner un nouveau souffle.

LE GARDIEN DE BUT DU REAL MADRID DEVRAIT-IL PORTER LE NUMÉRO 1 ?

Si les joueurs phares du Real portent des nombres premiers, quel numéro devrait alors figurer sur le maillot du gardien ? Autrement dit, en termes mathématiques, le 1 est-il un nombre premier ? Eh bien, oui et non. (Enfin une question mathématique sympathique : les deux réponses sont justes.) Il y a deux cents ans, la table des nombres premiers comprenait le 1 en première position. Après tout, il n'est pas divisible puisque le seul nombre entier qui le divise est lui-même. Aujourd'hui, cependant, le 1 n'est plus envisagé comme premier car les nombres premiers sont considérés avant tout comme les blocs de construction des nombres. Si je multiplie un nombre par un nombre premier, j'obtiens un nouveau nombre. Alors que si je multiplie un nombre par 1, je garde le même nombre. C'est donc sur cette base que nous excluons le 1 de la liste des nombres premiers et commençons par 2.

Évidemment, les dirigeants du Real n'ont pas été les premiers à découvrir la puissance des nombres premiers. Mais qui fut donc le premier, quelle civilisation ? Les Grecs anciens ? Les Chinois ? Les Égyptiens ? La vérité, c'est que les mathématiciens ont tous été coiffés au poteau par un étrange petit insecte.

COMMENT EXPLIQUER L'AFFECTION QUE PORTENT LES CIGALES AU NOMBRE PREMIER 17 ?

Dans les forêts de l'Amérique du Nord vit une espèce de cigale dont le cycle de vie est très étrange. Pendant 17 ans, ces cigales restent enfouies sous la terre à ne rien faire excepté sucer la sève des racines des arbres. Puis, au mois de mai de la 17^e année, elles émergent en masse et envahissent la forêt : presque deux millions par hectare.

Lorsque les cigales chantent, dans le but d'attirer un partenaire, elles produisent un tel bruit que bien des habitants préfèrent quitter les lieux le temps de l'invasion. C'est cette cacophonie assourdissante aux abords de la forêt proche de l'université de Princeton, où il recevait en 1970 un diplôme honorifique, qui inspira à Bob Dylan la chanson *Day of the Locusts*.

Lorsque la cigale mâle a attiré et fécondé une femelle, celle-ci pond environ 600 œufs dans les arbres. Puis, après six semaines de festivités, toutes les cigales trépassent et la forêt plonge dans un long, très long, silence. Vers le milieu de l'été, les œufs éclosent, puis les larves tombent au sol et s'enfoncent dans la terre jusqu'à ce qu'elles trouvent une racine capable de les sustenter pendant les 17 années qu'il faudra attendre avant leur prochaine grande fiesta.

Le fait que ces cigales soient capables de calculer un laps de temps de 17 années est un exploit d'ingénierie biologique extraordinaire. Il est très rare qu'elles sortent du sol en avance ou en retard. La plupart des animaux et des plantes obéissent à un cycle annuel régulé par les changements de température et de saison. Or, rien de tangible n'indique aux cigales que la Terre a fait 17 fois le tour du Soleil...

Pour le mathématicien, le plus curieux est le nombre d'années : 17, un nombre premier. Est-ce une coïncidence si ces cigales passent un nombre premier d'années enfouies sous terre ? Il

semblerait que non. D'autres espèces de cigale passent 13 ans sous le sol, et d'autres encore n'y séjournent que 7 ans. Toujours des nombres premiers. De manière assez étonnante, lorsqu'il advient qu'une cigale ayant un cycle de 17 ans sort de terre plus tôt, ce n'est pas avec une avance de 1 an, mais de 4 ans ; elle opte dans ce cas pour un cycle de 13 ans. Quelque chose qui concerne les nombres premiers aide vraisemblablement toutes ces espèces de cigale à s'y retrouver, mais quoi au juste ?

Bien que les scientifiques ne soient pas sûrs à 100 %, une théorie mathématique a été formulée pour expliquer l'addiction des cigales aux nombres premiers. Mais avant, voici quelques faits. Chaque forêt n'est peuplée que d'une seule sorte de cigale : le phénomène ne peut donc pas s'expliquer par la nécessité de partager les ressources entre différentes couvées. La plupart des années, il y a bien, quelque part sur le territoire nord-américain, une couvée de cigales qui apparaît et est « fan » d'un nombre premier. 2009 et 2010 furent des années sans aucune couvée. En revanche, en 2011, il y a eu une couvée massive de cigales de 13 ans dans le sud-est des États-Unis. (2011 est un nombre premier, mais je ne crois pas que les cigales soient à ce point intelligentes.)

La meilleure théorie à ce jour concernant le cycle de vie de la cigale est l'éventuelle existence d'un prédateur qui serait apparu lui aussi périodiquement dans la forêt, et aurait synchronisé son arrivée avec celle des cigales afin de transformer celles-ci en festin. C'est là que la sélection naturelle est intervenue : les cigales dont le cycle de vie correspond à un nombre premier rencontrent moins souvent des prédateurs que les autres, et survivent donc pour se reproduire, et ainsi de suite.



Fig. 1.02 L'interaction sur une période de 100 ans entre des populations de cigales ayant un cycle de vie de 7 ans et des prédateurs ayant un cycle de vie de 6 ans.

Par exemple, supposons que les prédateurs apparaissent tous les 6 ans. Les cigales qui émergent tous les 7 ans ne rencontrent les prédateurs que tous les 42 ans. En revanche, les cigales qui émergent tous les 8 ans auront affaire aux prédateurs tous les 24 ans ; et celles dont le cycle est de 9 ans, tous les 18 ans.

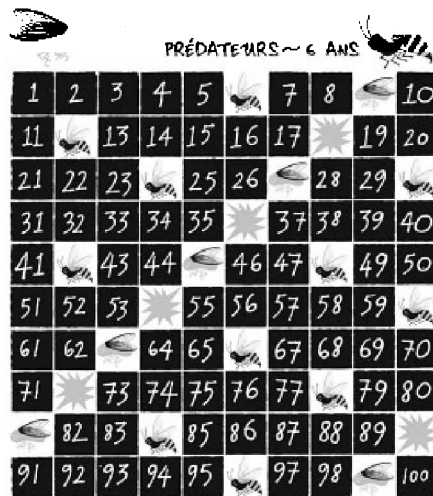


Fig. 1.03 L'interaction sur une période de 100 ans entre des populations de cigales ayant un cycle de vie de 9 ans et des prédateurs ayant un cycle de vie de 6 ans.

CIGALES CONTRE PRÉDATEURS

Téléchargez le fichier PDF du jeu de la cigale depuis la page Web dédiée au présent ouvrage. Découpez les prédateurs et les deux familles de cigales. Placez les prédateurs sur les nombres dans la table des 6. Chaque joueur prend une famille de cigales. Il vous faudra trois dés ordinaires à six faces. Le résultat du lancer de dés indique à quelle fréquence votre famille de cigales surgit de terre. Par exemple, si vous obtenez un 8, alors placez les cigales sur tous les nombres dans la table de 8. Mais si un prédateur se trouve déjà sur un de ces nombres, vous ne pouvez pas y placer une cigale — par exemple, vous ne pouvez pas mettre une cigale sur le 24 car la case est déjà occupée par un prédateur. Le gagnant est celui qui a le plus de cigales sur le plateau. En choisissant un autre nombre que 6 pour la périodicité du prédateur, vous pouvez créer une variante à ce jeu.

Il semblerait qu'il y ait donc eu dans les forêts d'Amérique du Nord une réelle compétition pour trouver le nombre premier qui permettrait d'éviter la sinistre rencontre avec les prédateurs. Les cigales y sont si bien parvenues que ces derniers sont soit morts de faim, soit partis ailleurs, laissant les cigales à leur étrange cycle de vie. Mais elles ne sont pas les seules à avoir exploité le rythme syncopé des nombres premiers. Lisez plutôt.

EN QUOI LES NOMBRES PREMIERS 17 ET 29 SONT-ILS LA CLÉ DE LA FIN DU TEMPS ?

Pendant la Seconde Guerre mondiale, le compositeur français Olivier Messiaen fut incarcéré en tant que prisonnier de guerre au stalag VIII-A, à Görlitz, où parmi les détenus il fit la rencontre d'un clarinettiste, d'un violoncelliste et d'un violoniste. Il décida de composer un quatuor pour ces trois musiciens, étant lui-même au piano. Il en résulta un des chefs-d'œuvre musicaux du XX^e siècle, *Quatuor pour la fin du temps*, qui fut présenté pour la toute première fois aux prisonniers et aux officiers du stalag VIII-A, avec Messiaen jouant sur un piano droit de fortune trouvé dans le camp.

Dans le premier mouvement, appelé « Liturgie de cristal », Messiaen souhaitait créer un sentiment de temps sans fin, et les nombres premiers 17 et 29 se révélèrent parfaits pour cela. Tandis

que le violon et la clarinette évoquent des chants d'oiseaux, le violoncelle et le piano fournissent la structure rythmique. Le piano joue une séquence rythmique, composée de 17 notes, ou valeurs, répétée tout au long du mouvement ; cette séquence est également fondée sur un retour périodique de 29 accords. Ainsi, lorsque la séquence rythmique de 17 notes commence pour la deuxième fois, la suite des accords n'est entamée qu'aux deux tiers. Le choix des nombres premiers 17 et 29 a pour conséquence que la séquence rythmique et la suite d'accords ne se « répètent » pas avant que 17×29 notes du morceau soient jouées.

Le caractère sans cesse changeant de la musique produit le sentiment d'intemporalité que Messiaen recherchait, et tout cela en utilisant la même astuce que celle des cigales pour déjouer leurs prédateurs. Il suffit d'envisager les cigales comme étant le rythme et les prédateurs les accords. Par leur différence, ces deux nombres premiers garantissent la non-synchronisation des deux séquences et le mouvement s'achève avant même que vous ayez pu entendre la musique se répéter.



Fig. 1.04 La « Liturgie de cristal », premier mouvement du *Quatuor pour la fin du temps* de Messiaen. La première ligne verticale indique où se termine la séquence rythmique composée de 17 valeurs. La seconde ligne indique le moment où s'achève la séquence harmonique composée d'une suite de 29 accords.

Messiaen ne fut pas le seul compositeur à utiliser les nombres premiers dans le domaine de la musique. Alban Berg s'est également servi d'un nombre premier comme signature dans sa musique. Tout comme David Beckham, Berg s'identifiait au numéro 23 — à vrai dire, ce chiffre l'obsédait. Par exemple, dans

Suite lyrique, des séquences de 23 mesures forment la structure du morceau que Berg a serti d'éléments représentant la liaison qu'il entretenait avec une femme mariée. Ainsi, sa maîtresse était évoquée par une séquence de 10 mesures entrelacée dans les 23 mesures qui symbolisaient le compositeur. Ce faisant, Berg a combiné mathématiques et musique pour donner vie à son histoire d'amour.

Tout comme les nombres premiers furent mis à contribution par Messiaen dans son *Quatuor pour la fin du temps*, les mathématiques ont récemment été utilisées pour créer un morceau qui, bien que n'étant pas intemporel, ne se répétera cependant pas avant mille ans. Pour célébrer l'arrivée du nouveau millénaire, Jem Finer, un des membres fondateurs des Pogues, eut l'idée de créer une installation musicale dans l'East End de Londres qui ne se répéterait pour la première fois qu'au tournant du prochain millénaire, en 3000. Son titre, *Longplayer*, ne pouvait être mieux choisi.

Finer a commencé avec un morceau de musique créé avec des bols chantants et des gongs tibétains de différentes tailles. La séquence musicale initiale dure 20 minutes et 20 secondes, et grâce à l'utilisation d'éléments mathématiques analogues aux astuces employées par Messiaen, il est parvenu à étendre son morceau pour le faire durer 1 000 ans. Six copies de la séquence initiale sont diffusées simultanément mais à des vitesses différentes. De plus, toutes les 20 secondes, chaque piste redémarre à une distance donnée par rapport au play-back original, mais cette distance est différente pour chaque piste. Le calcul mathématique à la base de ce décalage imposé à chaque piste garantit que les pistes ne s'aligneront jamais parfaitement durant un laps de temps de 1 000 ans.

Vous pouvez écouter *Longplayer* sur
<http://longplayer.org>

Les nombres premiers n'obsèdent pas uniquement les musiciens, ils sont aussi, semble-t-il, du goût de certains écrivains et réalisateurs de films. Par exemple, l'écrivain Mark Haddon n'a attribué que des nombres premiers aux chapitres de son roman *Le Bizarre Incident du chien pendant la nuit*. Christopher, le

personnage principal, est un jeune garçon atteint du syndrome d'Asperger, qui aime l'univers des mathématiques parce qu'il comprend comment celui-ci se comporte — la logique propre à ce monde-là signifie l'absence de surprises. Les interactions humaines, en revanche, sont trop remplies de ces incertitudes et illogismes que Christopher ne peut pas supporter en raison de son autisme. Comme il le dit lui-même : « J'aime les nombres premiers [...]. Je trouve que les nombres premiers sont comme la vie. Ils sont tout à fait logiques, mais il est impossible d'en trouver les règles, même si on consacre tout son temps à y réfléchir. »

Les nombres premiers ont même joué les vedettes au cinéma. Dans *Cube*, un thriller futuriste, sept personnages sont emprisonnés dans un labyrinthe de pièces qui ressemble à un Rubik's cube particulièrement compliqué. Chaque pièce, de forme cubique, a six portes donnant sur les autres pièces du labyrinthe. Au début du film, on voit les personnages se réveiller dans le cube, sans la moindre idée de ce qu'ils font là mais avec la certitude qu'ils doivent quitter ce lieu. Certaines pièces sont piégées, il leur faut déterminer lesquelles sont sûres et lesquelles ne doivent pas être empruntées pour leur éviter de mourir, que ce soit par le feu, l'acide ou même le fil à couper le beurre... comme ils le découvrent à mesure que leurs compagnons de malheur se font ainsi massacrer.

Un des personnages, une femme nommée Joan, est un génie des mathématiques qui réalise soudain que le chiffre figurant à l'entrée de chaque pièce doit permettre de déterminer si celle-ci est piégée ou non. Vraisemblablement, les pièces portant un nombre premier sont piégées. Impressionné par cette déduction mathématique, le chef du groupe loue « la beauté du cerveau » de Joan ; cependant, le groupe s'aperçoit très vite qu'il faut également faire attention aux puissances de nombres premiers ; là, même Joan est dépassée. Leur seul espoir repose désormais sur un autiste savant qui sera, au final, le seul à sortir vivant du labyrinthe...

Les cigales l'ont compris : les mathématiques aident parfois à rester en vie ! Les profs de mathématiques qui ont du mal à motiver leurs élèves ne devraient pas hésiter à se servir de *Cube* et des histoires de morts atroces qui se déroulent dans le film pour les convaincre de la nécessité d'étudier les nombres premiers et leur beauté.

POURQUOI LES AUTEURS DE SCIENCE-FICTION AIMENT-ILS LES NOMBRES PREMIERS ?

Lorsque les auteurs de SF ont besoin de faire communiquer leurs extraterrestres avec la planète Terre, un problème se pose à eux. Doivent-ils partir du principe que leurs extraterrestres sont assez futés pour avoir appris la langue du coin ou mis au point un traducteur capable d'interpréter nos propos ? Ou bien estiment-ils tout simplement que l'univers entier parle anglais ?

Une solution à ce problème, qui semble avoir séduit nombre d'auteurs de SF, repose sur l'idée que les mathématiques sont le seul langage véritablement universel, et que les premiers mots à connaître dans cette langue sont ses blocs de construction — les nombres premiers. Dans *Contact*, le roman de Carl Sagan, le personnage principal, Ellie Arroway, chercheuse à l'institut SETI (Search for Extra-Terrestrial Intelligence), tombe sur un signal qui n'est visiblement pas un bruit de fond mais une séquence de pulsations. Elle émet l'hypothèse qu'il s'agit de nombres représentés sous forme binaire. Ensuite, lorsqu'elle les traduit en nombres décimaux, un motif apparaît soudain : 59, 61, 67, 71... uniquement des nombres premiers. Et comme on pouvait s'y attendre, le signal se poursuit en listant tous les nombres premiers jusqu'à 907. Impossible que cela soit dû au hasard, conclut-elle. Quelqu'un est en train de dire bonjour.

De nombreux mathématiciens estiment qu'à l'autre bout de l'univers il y a une biologie, une chimie et même une physique différentes mais que les mathématiques, elles, sont les mêmes. N'importe qui, assis sur une planète en orbite autour de Véga en train de lire un livre de mathématiques consacré aux nombres premiers, considérera 59 et 61 comme des nombres premiers car, comme a pu le dire le célèbre mathématicien professeur à Cambridge G.H. Hardy, un nombre premier est premier « non parce que nous le pensons, ou parce que notre esprit est constitué d'une certaine manière, mais parce que c'est ainsi, parce que la réalité mathématique est ainsi ».

Bien que les nombres premiers soient sans doute communs à tout l'univers, il n'en demeure pas moins intéressant de se demander si on raconte dans d'autres mondes les mêmes genres d'histoires que celles que j'ai citées. La manière dont nous avons étudié ces nombres au cours du dernier millénaire nous a permis

de découvrir leurs propriétés. Et, à chacune des étapes de ce processus de découverte, nous pouvons voir la marque d'une perspective culturelle particulière, les motifs mathématiques propres à ce moment précis de l'histoire. D'autres civilisations dans l'univers ont-elles développé des perspectives différentes leur permettant d'accéder à des théorèmes qui nous sont inconnus ?

Carl Sagan n'était pas le premier et il ne sera pas le dernier à proposer l'utilisation des nombres premiers comme moyen de communication. Les nombres premiers ont même été utilisés par la NASA pour tenter d'établir le contact avec une intelligence extraterrestre. En 1974, le radiotélescope d'Arecibo à Puerto Rico a envoyé un message vers l'amas globulaire M13, choisi pour son impressionnant nombre d'étoiles dans le but d'augmenter les chances que le message tombe dans des oreilles intelligentes. Le message était composé d'une série de 0 et de 1 qui pouvaient être agencés de manière à former une image pixélisée en noir et blanc. L'image reconstituée montre, entre autres, les nombres de 1 à 10 en format binaire, la structure de l'ADN, notre système solaire et une image du radiotélescope d'Arecibo lui-même. Étant donné qu'il n'y avait que 1 679 pixels, l'image n'est pas très détaillée mais ce choix du nombre 1 679 était volontaire car il contient la clé de la disposition des pixels. 1 679 est le produit de deux nombres premiers, 23 et 73. Il n'y a donc que deux manières d'agencer les pixels dans un rectangle pour fabriquer l'image : 23 rangées et 73 colonnes, mais cela ne produit rien d'intelligible ; ou bien 73 rangées et 23 colonnes, ce qui donne l'image souhaitée. La constellation M13 étant à 25 000 années-lumière de la Terre, nous attendons encore une réponse. Et il nous faudra patienter encore un peu, disons environ 50 000 années !



Fig. 1.05 Le message diffusé par le radiotélescope d'Arecibo vers l'amas globulaire M13.

Bien que les nombres premiers soient universels, la manière dont nous les écrivons a beaucoup varié au cours de l'histoire des mathématiques, en fonction notamment de spécificités culturelles — comme ce petit tour du monde va nous le montrer.

DE QUEL NOMBRE PREMIER S'AGIT-IL ?

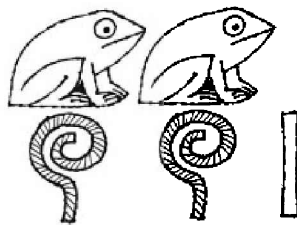


Fig. 1.06

Certains des premiers éléments mathématiques de l'histoire sont apparus dans l'Égypte ancienne. Voici comment les Égyptiens écrivaient le nombre 200 201 sous l'Antiquité. Dès 6000 ans av. J.-C., des peuples commencèrent à abandonner la vie nomade pour se sédentariser le long des rives du Nil. Puis, lorsque la société égyptienne devint plus sophistiquée, on eut besoin de plus en plus

de nombres pour tenir les registres des impôts, mesurer les champs et construire les pyramides. L'écriture des nombres reposait sur le même système de hiéroglyphes que celui de la langue. Il est intéressant de constater que les Égyptiens avaient inventé un système de numération fondé sur les puissances de 10, comme notre système décimal actuel. (Ce choix ne procède pas d'une quelconque signification mathématique du nombre 10, mais du simple fait que nous avons dix doigts.) Cependant il leur restait encore à inventer le système de position, où la place d'un nombre est reliée à une puissance de 10 ou d'un autre nombre fixe. Selon le système de position, par exemple, les 2 dans le nombre 222 ont chacun une valeur différente selon leur position. N'ayant pas trouvé ce système, les Égyptiens auront besoin d'un symbole différent pour chaque nouvelle puissance de 10 :

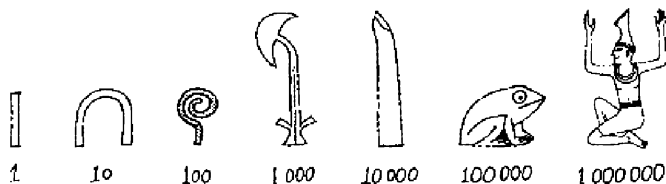


Fig. 1.07 Symboles utilisés en Égypte ancienne pour les puissances de 10. 10 est un os de talon stylisé, 100 une corde et 1 000 un lotus.

200 201 peut s'écrire avec seulement cinq symboles, mais combien en faut-il pour écrire le nombre premier 9 999 991 en hiéroglyphes ? Il vous faudra 55 symboles. Même si les Égyptiens n'avaient pas encore pris conscience de l'importance des nombres premiers, ils développèrent néanmoins plusieurs principes mathématiques sophistiqués, notamment — oh, surprise — la formule pour calculer le volume d'une pyramide et une notion de fractions. Mais leur système de notation des nombres était plutôt rudimentaire comparé à celui de leurs voisins, les Babyloniens.

DE QUEL NOMBRE PREMIER S'AGIT-IL ?

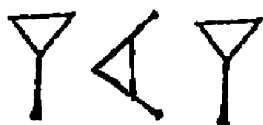


Fig. 1.08

Voici comment les Babyloniens écrivaient le nombre 71. Tout comme l'Empire égyptien, l'Empire babylonien s'étendait tout autour d'un grand fleuve, l'Euphrate. À partir de 1800 av. J.-C., les Babyloniens prirent possession de la majeure partie de l'Irak, de l'Iran et de la Syrie actuels, une expansion et un développement qui nécessitèrent une parfaite maîtrise de la manipulation et du traitement des nombres. Des registres étaient consignés sur des tablettes d'argile par des scribes qui utilisaient un bâton en bois ou stylet pour tracer des marques dans le matériau encore humide avant de mettre les tablettes à sécher. La pointe du stylet était cunéiforme (en forme de clou) — d'où le nom donné à cette écriture.

Vers 2000 av. J.-C., les Babyloniens devinrent une des premières civilisations à utiliser le système de numération positionnel. Mais au lieu de fonder le système sur les puissances de 10 comme les Égyptiens, les Babyloniens développèrent un système positionnel en base 60. Ils utilisaient différentes combinaisons de symboles pour exprimer les nombres de 1 à 59, et lorsqu'ils atteignaient 60, ils commençaient une nouvelle colonne « 60 » à gauche de la précédente et enregistraient la présence d'un lot de 60, tout comme dans le système décimal nous plaçons un 1 dans la colonne des dizaines quand les unités dépassent 9. Ainsi, le nombre premier illustré ci-dessus consiste en un lot de 60 accompagné du symbole pour 11, ce qui fait 71. Notons que les symboles des nombres jusqu'à 59 ne sont pas sans lien avec le système décimal puisque les nombres de 1 à 9 sont représentés par des lignes horizontales, mais ensuite 10 est représenté par le symbole suivant :



Fig. 1.09

Le choix de la base 60 est beaucoup plus judicieux mathématiquement que celui de la base 10 de notre système décimal. En effet, 60 a de nombreux diviseurs, ce qui facilite grandement les calculs. Par exemple, si j'ai 60 haricots, je peux les diviser d'une multitude de façons différentes :

$$60 = 30 \times 2 = 20 \times 3 = 15 \times 4 = 12 \times 5 = 10 \times 6$$

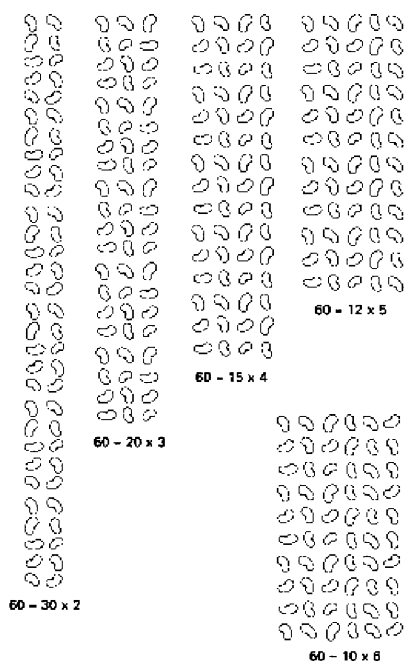


Fig. 1.10 Les différentes manières de répartir 60 haricots.

Les Babyloniens faillirent découvrir un chiffre très important en mathématiques : le zéro. Si on veut écrire en cunéiforme le nombre premier 3 607, on rencontre un problème car cela fait un lot de 3 600, ou 60 au carré, et 7 unités. Or, si on écrit cela tel quel, on

court le risque que cela ressemble à un lot de 60 et 7 unités — certes toujours un nombre premier, mais pas le bon. Pour résoudre ce problème, les Babyloniens conçurent un petit symbole afin d'indiquer qu'il n'y avait pas de 60 à compter dans la colonne des 60. De la sorte, 3 607 pouvait s'écrire ainsi :

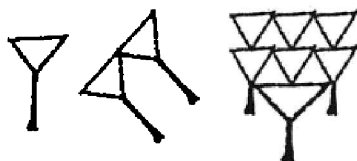


Fig. 1.11

Pour autant donc, ils n'envisagèrent pas le zéro comme un nombre de plein droit. Pour eux, il s'agissait juste d'un symbole propre à leur système positionnel exprimant l'absence de telle ou telle puissance de 60, c'est-à-dire d'un marqueur d'absence. Les mathématiques allaient devoir attendre encore 2 700 ans, soit jusqu'au VII^e siècle de notre ère, pour que les Indiens introduisent le zéro et explorent les propriétés de ce chiffre.

Non seulement les Babyloniens développèrent une manière sophistiquée d'écrire les nombres, mais c'est également à eux que l'on doit la découverte de la première méthode pour résoudre les équations du second degré, chose que tout collégien actuel apprend à faire à l'école. Ils étaient également sur la piste du théorème de Pythagore concernant les triangles rectangles. En dépit de tout cela, nous n'avons aucune véritable preuve que les Babyloniens appréciaient la beauté des nombres premiers.

COMMENT COMPTER JUSQU'À 60 AVEC SES DOIGTS

Nous avons hérité de nombreux vestiges de la base 60 utilisée par les Babyloniens. Par exemple, les 60 secondes d'une minute et les 60 minutes d'une heure, sans oublier les 360 degrés ($3 \times 60^\circ$) d'un cercle.

Il semblerait en outre que les Babyloniens aient utilisé leurs doigts pour compter jusqu'à 60 d'une manière plutôt astucieuse. Nos doigts (à l'exception du pouce) ont chacun trois phalanges. Le pouce d'une main peut toucher chacune de ces phalanges. La main gauche sert à compter jusqu'à 12, tandis que les quatre doigts de la main droite sont utilisés pour garder en mémoire le nombre de lots de 12 comptés. Au total, il est possible de compter jusqu'à cinq lots de 12 (quatre lots de 12 sur la main droite plus un lot de 12 compté sur la main gauche), c'est-à-dire jusqu'à 60.

Par exemple, pour compter le nombre premier 29, il faut toucher l'auriculaire puis l'annulaire de la main droite (soit 24) et avec l'autre main toucher du pouce la cinquième phalange, c'est-à-dire celle au milieu du majeur (soit 5).

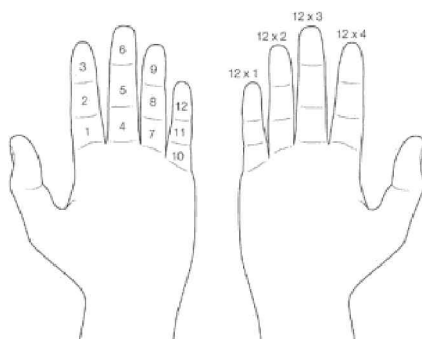


Fig. 1.12

DE QUEL NOMBRE PREMIER S'AGIT-IL ?



Fig. 1.13

La culture méso-américaine des Mayas connut son apogée de 200 à 900 av. J.-C. Elle s'étendait du sud du Mexique au Guatemala et au Salvador. Les Mayas possédaient un système de numération sophistiqué qu'ils avaient développé pour faciliter leurs calculs astronomiques avancés ; et c'est ainsi qu'ils écrivaient le nombre 17. À la différence des Égyptiens et des Babyloniens, les Mayas opéraient en base 20. Un point servait à indiquer 1, deux points 2, et trois points 3. Exactement comme un prisonnier marque à la craie les jours sur les murs de sa cellule, une fois arrivés à 5, au lieu de faire le cinquième point, ils traçaient une ligne à travers les quatre points. Ainsi, une ligne, ou trait horizontal, exprime 5.

Il est intéressant de noter que ce système est fondé sur le principe que notre cerveau est capable de distinguer rapidement de petites quantités — il nous est facile de voir s'il y a une, deux, trois ou quatre choses —, en revanche, au-delà, nous avons plus de mal. Une fois que les Mayas ont compté jusqu'à 19 — trois traits surmontés de quatre points —, ils créent une nouvelle colonne afin de compter la quantité de 20 (les vingtaines). La colonne suivante aurait dû servir à indiquer la quantité de 400 (20×20) mais, bizarrement, cette colonne exprime combien il y a de 360 (20×18). Ce choix bizarre est lié aux cycles du calendrier maya. Un cycle se compose de 18 mois de 20 jours. Mais cela ne fait que 360 jours. Pour arriver à 365, les Mayas ont ajouté un mois de cinq « mauvais jours » dont, comme leur nom l'indique, on considérait qu'ils portaient malheur.

Tout comme les Babyloniens, les Mayas utilisaient un symbole spécial pour indiquer l'absence de certaines puissances de 20. Chaque position dans leur système de numération était associée à une divinité, et il était considéré comme irrespectueux de ne rien donner à « tenir » à un dieu, ainsi un glyphe en forme de coquillage était utilisé pour signifier l'absence. La création de ce symbole pour dénoter l'absence provient de considérations tout autant superstitieuses que mathématiques. Comme les Babyloniens, les

Mayas ne concevaient toujours pas zéro comme un nombre à part entière.

Si les Mayas développèrent un système de numération permettant de compter jusqu'à de très grands nombres, c'est que leurs calculs astronomiques englobaient de gigantesques cycles de temps. Un cycle de temps est mesuré par ce qui s'appelle le Long Compte (dont le point de départ est le 11 août 3114 av. J.-C.). Il nécessite cinq « colonnes » ou positions, et atteint les $20 \times 20 \times 20 \times 18 \times 20$ jours, ce qui fait un total de 7 890 années. Le 21 décembre 2012 s'écrit 13.0.0.0 dans le calendrier maya. Comme des gamins qui fixent du regard le compteur kilométrique d'une voiture alors que le passage au millier suivant est imminent, les Guatémaltèques vécurent cet événement avec un mélange d'excitation et d'appréhension. Ceux qui prédisaient la fin du monde à cette date ont pu constater leur erreur.

DE QUEL NOMBRE PREMIER S'AGIT-IL ?



Fig. 1.14

Bien qu'il s'agisse de lettres et non de chiffres, c'est ainsi que le nombre 13 s'écrit en hébreu. Dans la tradition juive de la gematria, les lettres de l'alphabet hébreu ont chacune une valeur numérique. Ici, *gimel* est la troisième lettre de l'alphabet et *yod* la dixième ; cette combinaison de lettres représente donc le nombre 13. La table 1.01 donne les valeurs numériques de chacune des lettres.

Les kabbalistes aiment jouer avec les valeurs numériques des mots et voir les liens et interprétations qui peuvent en surgir. Par exemple, mon prénom a comme valeur numérique :

<i>mem</i>		<i>resh</i>		<i>kaf</i>		<i>vav</i>		<i>samech</i>	
40	+	200	+	20	+	6	+	60	= 326

c'est-à-dire la même valeur numérique que les mots « *man of fame* » (homme célèbre)... ou que « *asses* » (imbéciles), par exemple. Selon certains, si 666 est le nombre de la Bête, c'est qu'il correspond à la valeur numérique de Néron, un des plus sanguinaires empereurs romains de l'histoire.

<i>Alphabet hébreu</i>	<i>Équivalent français</i>	<i>Valeur numérique</i>
א, aleph	A	1
ב, beth	B	2
ג, gimel	G	3
ד, dalet	D	4
ה, he	H, E	5
ו, vav	V, U, O	6
ז, zayin	Z	7
ח, het	Ch	8
ט, tet	T	9
י, yod	I, Y, J	10
כ, kaf	K	20
ל, lamed	L	30
מ, mem	M	40
נ, nun	N	50
ס, samech	S	60
ע, ayin	O, Ng	70
פ, pe	P	80
צ, tsade	Tz	90
ק, qof	Q	100
ר, resh	R	200
ש, shin	Sh	300
ת, tav	Th	400

Table 1.01

Vous pouvez calculer la valeur de votre nom en additionnant les valeurs numériques de la table 1.01. Pour voir quels autres mots hébreux ont la même valeur numérique que votre nom, allez sur <http://bit.ly/Heidrick>.

Bien que les Hébreux n'accordent pas de signification particulière aux nombres premiers, il n'en est pas de même pour les nombres parfaits. De quoi s'agit-il ? Prenez un nombre, et regardez tous les nombres qui le divisent (sauf le nombre de départ lui-même). Si, en additionnant tous ces diviseurs, vous obtenez le nombre de départ, alors celui-ci s'appelle un nombre parfait. Le premier nombre parfait est 6. Ses diviseurs sont 1, 2 et 3 (on ne tient pas compte du diviseur 6). Additionnez-les ($1 + 2 + 3$) et vous obtenez 6. Le nombre parfait suivant est 28. Les diviseurs de 28 sont 1, 2, 4, 7 et 14 qui, une fois additionnés, font 28. Selon la religion juive, le monde a été construit en six jours et, selon le calendrier hébraïque, le mois lunaire compte 28 jours. Voilà pourquoi dans la culture juive on estime que les nombres parfaits revêtent une signification spéciale.

Les propriétés mathématiques et religieuses des nombres parfaits furent également remarquées par les commentateurs chrétiens. Dans son célèbre texte *La Cité de Dieu*, saint Augustin (354-430) écrivait : « Six est un nombre parfait en lui-même, non parce que Dieu a créé toutes choses en six jours, mais Dieu a créé toutes choses en six jours parce que ce nombre est parfait. »

Parmi ces nombres parfaits se cachent des nombres premiers. Chaque nombre parfait correspond à une sorte particulière de nombre premier, le « nombre premier de Mersenne » (nous y reviendrons plus loin dans ce chapitre). À ce jour, nous ne connaissons que 47 nombres parfaits. Le plus grand comporte 25 956 377 chiffres. Tout nombre parfait pair est de la forme $2^n - 1(2^n - 1)$. Et lorsque $2^n - 1(2^n - 1)$ est parfait, alors $2^n - 1$ sera un nombre premier, et inversement. Nous ne savons pas à ce jour s'il existe des nombres parfaits impairs.

DE QUEL NOMBRE PREMIER S'AGIT-IL ?

二十三

Fig. 1.15

Vous pensez peut-être qu'il s'agit du nombre premier 5 ; il est vrai qu'on dirait $2 + 3$. Cependant, le symbole 十 ne désigne pas le signe +, mais le caractère chinois pour 10. Ensemble, les trois caractères indiquent deux lots de 10 et trois unités, soit 23.

Cette forme traditionnelle de numération chinoise ne reposant pas sur un système positionnel, des symboles étaient utilisés pour exprimer les différentes puissances de 10. Un tout autre système de numération exprimant les chiffres à l'aide de bâtons de bambou était, lui, un système de position et s'inspirait de l'abaque, sur lequel, lorsque 10 est atteint, on commence une nouvelle colonne.

Voici les chiffres de 1 à 9 en bâtons de bambou :

—	=	≡	≡	≡	⊥	⊥	⊥	⊥
1	2	3	4	5	6	7	8	9

Fig. 1.16

Afin d'éviter toute confusion, dans une colonne sur deux (celle des dizaines, des milliers, des centaines de milliers, etc.), le sens des bâtons de bambou était inversé (les traits verticaux devenant horizontaux et inversement) :

					⊥	⊥	⊥	⊥
1	2	3	4	5	6	7	8	9

Fig. 1.17

Les Chinois anciens avaient même un concept de nombre négatif, qu'ils représentaient grâce à des bâtons de couleurs différentes. On pense que l'utilisation du noir et du rouge dans la

comptabilité occidentale trouve son origine dans la pratique chinoise d'utilisation de bâtons rouges et noirs, même si les Chinois, eux, utilisaient le noir pour signifier les nombres négatifs...

La Chine est probablement l'une des premières civilisations à accorder de l'importance aux nombres premiers. Les Chinois pensaient que chaque nombre avait son propre genre sexué — les nombres pairs étaient féminins, les impairs masculins. Ils constatèrent cependant que certains nombres impairs étaient particuliers. Par exemple, si vous avez 15 cailloux, il est possible de les agencer pour former un beau rectangle, en trois rangées de cinq. Mais si vous avez 17 cailloux, il n'est pas possible de les agencer de manière parfaitement ordonnée : on ne peut que les ranger à la suite pour former une ligne droite. Pour les Chinois, les nombres premiers étaient donc les seuls nombres véritablement virils. Et, bien que masculins, les nombres impairs ne faisant pas partie des nombres premiers étaient considérés comme efféminés.

Les Chinois anciens mettaient ainsi en valeur la propriété fondamentale des nombres premiers, car le nombre de cailloux dans une pile est premier s'il n'y a aucun moyen de les agencer pour former un vrai rectangle digne de ce nom.

Nous avons vu comment, pour représenter des nombres, les Égyptiens utilisaient des glyphes de grenouilles, les Mayas dessinaient des points et des traits, les Babyloniens traçaient dans l'argile des marques en forme de clou, les Chinois disposaient des bâtons, et comment, dans la culture hébraïque, les lettres de l'alphabet servent à représenter des nombres. Bien que les Chinois fussent sans doute les premiers à accorder quelque importance aux nombres premiers, c'est une autre civilisation qui s'approcha des mystères de ces nombres énigmatiques : les Grecs anciens.

COMMENT LES GRECS PASSÈRENT AU CRIBLE LES NOMBRES PREMIERS

Voici un moyen systématique découvert par les Grecs anciens qui est très efficace pour trouver les nombres premiers pas trop grands. Cette méthode procède par élimination de tous les nombres non premiers. Écrivez les nombres de 1 à 100. Commencez par

barrer le nombre 1. (Comme je l'ai déjà dit, au temps des Grecs, 1 était considéré comme un nombre premier mais ce n'est plus le cas aujourd'hui.) Passez au nombre suivant, le 2. Voici le premier nombre premier. Barrez maintenant tous les nombres de 2 en 2 après 2 ; cela revient à barrer tous les nombres pairs à l'exception de 2.



Fig. 1.18 Barrez un nombre sur deux après 2.

Maintenant, prenez le nombre le plus petit qui n'a pas été barré, c'est le 3, et barrez systématiquement tous les nombres qui sont dans la table de 3 sauf 3 :



Fig. 1.19 Maintenant barrez chaque troisième nombre à partir du 3.

Comme le 4 a déjà été barré, on passe au nombre suivant, le 5, et on barre de 5 en 5 à partir de 5. Nous répétons ce processus en revenant chaque fois au plus petit nombre n qui n'a pas encore été barré, et ensuite nous barrons, en avançant, tous les nombres à une distance n de lui :

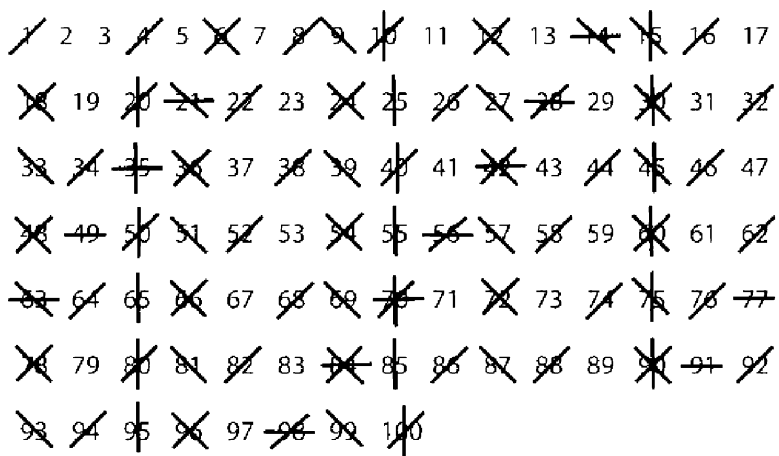


Fig. 1.20 Voilà, il ne reste que les nombres premiers de 1 à 100.

La beauté de ce processus est qu'il est tout à fait automatique — sa mise en œuvre ne requiert pas beaucoup de réflexion. Par exemple, 91 est-il un nombre premier ? Grâce à cette méthode, nul besoin de réfléchir. 91 a été barré lorsque nous avons rayé tous les nombres de 7 en 7 à partir de 7, car $91 = 7 \times 13$. Les gens se trompent souvent avec 91, car il est rare d'apprendre la table de 7 jusqu'à 13.

Ce procédé systématique est un bon exemple d'algorithme, une méthode de résolution de problème fondée sur l'application d'une série spécifique d'instructions — définition qui s'applique aussi aux programmes informatiques. Cet algorithme particulier fut découvert il y a deux millénaires dans un des principaux foyers de l'activité mathématique d'alors, la ville d'Alexandrie (aujourd'hui en Égypte). À cette époque, Alexandrie était un des avant-postes du grand Empire grec et possédait une des plus fabuleuses bibliothèques au monde. C'est au cours du III^e siècle av. J.-C. que le savant Ératosthène, qui dirigeait la célèbre bibliothèque, conçut cette méthode (ancêtre des programmes informatiques) pour identifier les nombres premiers.

Cette méthode s'appelle le crible d'Ératosthène, car chaque fois que vous barrez un groupe de nombres non premiers, c'est comme si vous vous serviez d'un crible et que vous régliez les intervalles en fonction de chaque nouveau nombre premier que vous allez traiter. D'abord, vous utilisez un tamis avec des fils de fer à un intervalle de 2, puis de 3, puis de 5. Et ainsi de suite. Malheureusement, cette méthode perd rapidement de son efficacité lorsque vous cherchez des nombres premiers très grands.

Outre qu'il passa au crible les nombres premiers et prit en charge des centaines de milliers de rouleaux de papyrus et de vélin de la bibliothèque, Ératosthène calcula la circonférence de la Terre ainsi que la distance de la Terre au Soleil et celle de la Terre à la Lune. Selon ses calculs, le Soleil se trouvait à 804 000 000 de stades de la Terre, mais son unité de mesure rend la vérification de l'exactitude de son calcul un peu difficile. De quelle taille est le stade que nous sommes supposés utiliser : Wembley, ou quelque chose de plus petit comme Loftus Road ?

En plus d'avoir mesuré le système solaire, Ératosthène définit le tracé du Nil et fut le premier à expliquer pourquoi il débordait régulièrement : les pluies diluviennes à sa source lointaine en Éthiopie en étaient la cause. Ératosthène était également poète. Malgré toutes ces activités, ses amis le surnommèrent Bêta — parce qu'il ne fit jamais rien de bon. On dit qu'il se laissa mourir de faim après qu'il fut devenu aveugle.

COMBIEN DE TEMPS FAUDRAIT-IL POUR FAIRE LA LISTE DE TOUS LES NOMBRES PREMIERS ?

Toute personne qui entreprendrait une telle tâche y passerait l'éternité car il y a une infinité de nombres premiers. Pourquoi sommes-nous si sûrs que jamais nous ne parviendrons au dernier nombre premier, qu'il y a, toujours, un autre nombre premier à ajouter à la liste ? C'est là un des grands exploits du cerveau humain : avec une simple séquence finie d'étapes logiques, nous pouvons saisir l'idée de l'infini.

Le mathématicien grec Euclide, un élève de Platon, fut le premier à démontrer qu'il y a une infinité de nombres premiers. Il

vécut à Alexandrie au III^e siècle tout comme Ératosthène, son cadet de cinquante ans.

Pour le démontrer, Euclide prit le problème à l'envers en se demandant si le nombre de nombres premiers n'était pas, en fait, fini. Cette liste finie de nombres premiers aurait comme propriété que tous les autres nombres devraient s'obtenir en multipliant entre eux les nombres premiers de ladite liste. Pour simplifier, admettons que vous pensiez que la liste de tous les nombres premiers comporte uniquement les trois nombres suivants : 2, 3 et 5. Tout nombre serait obtenu en multipliant 2, 3 et 5 de différentes manières. Euclide concocta une façon d'obtenir un nombre ne pouvant jamais être le produit exact de ces trois nombres premiers. Il commença par multiplier cette liste de nombres premiers pour obtenir 30. Puis — et c'est là son trait de génie —, il ajouta 1 à ce nombre pour faire 31. Aucun des nombres premiers de la liste, 2, 3 ou 5, ne le divise exactement. Il reste toujours 1.

Si tous les nombres sont construits en multipliant ces nombres premiers entre eux, que dire alors de 31 ? Comme ce nombre ne peut être divisé par 2, 3 ou 5, il doit exister d'autres nombres premiers, ne figurant pas sur cette liste, capables de produire 31. En fait, 31 est lui-même un nombre premier, donc Euclide avait créé un « nouveau » nombre premier. Il nous suffit simplement d'ajouter ce nouveau nombre premier à la liste, me direz-vous. Mais Euclide peut alors réitérer son astuce. Quelle que soit la taille de la table des nombres premiers, il lui suffit de multiplier la liste de nombres premiers et d'ajouter 1. On trouvera ainsi soit un nombre premier, soit un nombre divisible par un nombre premier ne se trouvant pas dans la liste. C'est ainsi qu'Euclide put affirmer qu'aucune liste finie ne contiendra jamais tous les nombres premiers. Par conséquent, il y a un nombre infini de nombres premiers.

Bien qu'Euclide apportât la preuve que les nombres premiers sont en nombre infini, sa démonstration comportait cependant un défaut — elle ne dit pas où sont les nombres premiers. Vous pensez peut-être que sa méthode produit une manière de générer de nouveaux nombres premiers. Après tout, lorsque nous avons multiplié 2, 3 et 5 ensemble et avons ajouté 1, nous avons obtenu 31, un nouveau nombre premier. Mais cela ne marche pas à chaque fois. Par exemple, regardez la liste de nombres premiers suivante : 2, 3, 5, 7, 11 et 13. Multipliez-les tous ensemble : 30 030. Maintenant ajoutez 1 à ce nombre : 30 031. Ce nombre n'est pas

divisible par les nombres premiers de 2 à 13, car on obtient toujours le reste 1. Cependant, il ne s'agit pas d'un nombre premier car il est divisible par deux nombres premiers, 59 et 509, et ils n'étaient pas sur notre liste. En fait, les mathématiciens ne savent toujours pas si le processus qui consiste à multiplier une liste finie de nombres premiers ensemble, puis d'y ajouter 1 infiniment souvent, permet de créer un nouveau nombre premier.

Dans cette vidéo de mon équipe de foot j'explique (en anglais) pourquoi les nombres premiers sont infiniment nombreux. Allez sur <http://bit.ly/Primenumbersfootball>

POURQUOI MES FILLES ONT-ELLES COMME DEUXIÈMES PRÉNOMS 41 ET 43 ?

S'il ne nous est pas possible d'inscrire les nombres premiers dans une seule grande table, peut-être pouvons-nous essayer de trouver un motif récurrent qui nous aiderait à générer des nombres premiers. Existe-t-il un moyen astucieux d'analyser les nombres premiers connus dans le but de déterminer où se trouve le suivant ?

Voici les nombres premiers découverts grâce au crible d'Ératosthène pour les nombres de 1 à 100 :

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53,
59, 61, 67, 71, 73, 79, 83, 89, 97

Il est très difficile de déterminer où se trouve le nombre premier suivant, car il ne semble pas y avoir dans la séquence de motif récurrent qui permette de le localiser. En fait, ces nombres ressemblent plus à des numéros sur des billets de loto qu'aux blocs de construction des mathématiques. C'est comme d'attendre le bus, parfois il y a un grand intervalle sans aucun nombre premier, puis soudain plusieurs arrivent les uns après les autres. Ce comportement est caractéristique des processus aléatoires, comme nous le verrons au chapitre 3.

À l'exception de 2 et 3, l'écart entre deux nombres premiers ne peut être inférieur à 2, comme 17 et 19 ou 41 et 43, car la

différence entre deux nombres premiers est toujours paire. Les couples de nombres premiers distants de 2 s'appellent des nombres premiers jumeaux. Étant obsédé par les nombres premiers, j'ai failli appeler mes jumelles 41 et 43 à leur naissance. Après tout, si Chris Martin et Gwyneth Paltrow ont appelé leur bébé Apple et si Frank Zappa a baptisé ses filles Moon Unit et Diva Thin Muffin Pigeon, pourquoi mes filles ne pourraient-elles pas porter les prénoms 41 et 43 ? Mais ma femme n'était pas très partante, je me suis donc contenté de donner ces deuxièmes prénoms « en secret » à mes filles.

Bien que les nombres premiers se raréfient à mesure que l'on s'éloigne dans la suite infinie des nombres, la fréquence avec laquelle surgissent des paires de nombres premiers jumeaux peut surprendre. Par exemple, après le nombre premier 1 129, il n'y a aucun nombre premier parmi les 21 nombres suivants, puis, soudain, on tombe sur une paire de nombres premiers jumeaux, 1 151 et 1 153. Et une fois qu'on a dépassé le nombre premier 102 701, il faut attendre encore 59 nombres non premiers pour voir apparaître la paire de nombres premiers jumeaux 102 761 et 102 763. Les plus grands nombres premiers jumeaux découverts, début 2011, ont 200 700 chiffres. Étant donné qu'un nombre ayant seulement 80 chiffres suffit pour décrire le nombre d'atomes dans l'univers observable, ces nombres sont d'une grandeur inouïe.

Existe-t-il d'autres jumeaux ensuite ? Grâce à la preuve d'Euclide, nous savons que nous allons trouver encore une infinité de nombres premiers, mais d'autres nombres premiers jumeaux y figureront-ils ? À ce jour, personne n'a formulé de belle démonstration comme celle d'Euclide pour démontrer l'existence d'une infinité de nombres premiers jumeaux.

Il y a quelques années, on a cru que des vrais jumeaux pouvaient être la clé du secret des nombres premiers. Dans son livre intitulé *L'Homme qui prenait sa femme pour un chapeau*, Oliver Sacks décrit le cas véridique de jumeaux autistes, des génies qui utilisaient entre eux les nombres premiers comme langage secret. Ils avaient pour habitude de se rendre à la clinique de Sacks où, assis dans son cabinet, ils échangeaient de grandes quantités de nombres. Au début, Sacks ne comprenait rien à leur dialogue mais, une nuit, il trouva le secret de leur code. Il fit quelques calculs avec des nombres premiers et décida de mettre sa théorie à l'épreuve. Le lendemain, assis aux côtés des jumeaux tandis qu'ils échangeaient des nombres à six chiffres, Sacks profita d'un moment de pause dans leur bavardage numérique pour lancer un nombre premier à

sept chiffres, prenant ainsi les frères par surprise. Ils réfléchirent en silence un moment, car cela dépassait tout de même la limite des nombres premiers qu'ils échangeaient jusqu'alors, puis soudain, exactement en même temps, ils sourirent comme s'ils reconnaissaient un ami.

Au fil des séances avec Sacks, ils échangèrent des nombres premiers ayant même jusqu'à neuf chiffres. Bien sûr, si leur dialogue avait été constitué de nombres impairs quelconques ou même de nombres carrés, personne n'aurait trouvé cela remarquable ; mais là, puisque les nombres premiers sont réputés pour être dispersés de manière aléatoire, il s'agissait d'un exploit extraordinaire. Il peut s'expliquer par une autre capacité dont jouissaient les jumeaux. Ils passaient souvent à la télévision et impressionnaient les téléspectateurs en établissant par exemple que le 23 octobre 1901 avait été un mercredi. Il est possible de trouver le jour de la semaine d'une date donnée grâce à un ensemble de méthodes appelé arithmétique modulaire ou parfois arithmétique de la montre. Peut-être les jumeaux avaient-ils découvert que l'arithmétique modulaire permettait également de savoir si un nombre est premier ?

Prenons un nombre, disons 17, et calculons 2^{17} : si, après division de ce nombre par 17, le reste est 2, nous avons là une preuve que 17 est un nombre premier. Bien que ce test de primalité (critère pour qu'un nombre soit premier) soit souvent attribué aux Chinois, c'est en réalité le mathématicien français du XVII^e siècle Pierre de Fermat qui prouva que si le reste n'est pas 2, cela implique que 17 n'est pas premier. D'une manière générale, si l'on souhaite vérifier que p n'est pas un nombre premier, alors on calcule 2^p et on divise le résultat par p . Si le reste n'est pas 2, alors p ne peut pas être un nombre premier. Selon certaines personnes, l'aptitude des jumeaux à identifier le jour de la semaine d'une date donnée est fondée sur une technique similaire d'analyse du reste après division par 7, et il est probable qu'ils utilisaient ce test pour trouver des nombres premiers.

Au début, les mathématiciens pensaient qu'inversement, si 2^p donne un reste de 2 après division par p , alors p doit être un nombre premier. Mais en fait, ce test ne garantit pas la primalité. $341 = 31 \times 11$ n'est pas un nombre premier, et pourtant 2^{341} donne le reste 2 après division par 341. Cet exemple ne fut découvert qu'en 1819, et il est possible que les jumeaux aient eu connaissance d'un test plus sophistiqué encore permettant de faire sortir 341 de

sa cachette. Fermat démontra que le test pouvait être étendu au-delà des puissances de 2 en prouvant que si p est un nombre premier, alors pour tout nombre n inférieur à p , n^p donne toujours un reste n lorsqu'il est divisé par le nombre premier p . Donc, si on trouve un nombre n pour lequel cela échoue, p est un imposteur et vous pouvez le jeter.

Par exemple, 3^{341} ne donne pas un reste de 3 après division par 341 — le reste est 168. Il est invraisemblable que les jumeaux aient vérifié tous les nombres inférieurs à leur nombre premier candidat : il y aurait eu bien trop de tests à effectuer. Cependant, le grand magicien des nombres premiers, le Hongrois Paul Erdős, estima (sans pouvoir le prouver de manière rigoureuse) que, lorsqu'on cherche à savoir si un nombre inférieur à 10^{150} est un nombre premier, il suffit de réussir le test de Fermat une seule fois pour que la probabilité que le nombre ne soit pas premier tombe à seulement 1 chance sur 10^{43} . Donc, pour les jumeaux, il est probable qu'un test suffisait pour leur donner le frisson de la découverte d'un nombre premier.

LA MARELLE DES NOMBRES PREMIERS

Il s'agit d'un jeu pour deux joueurs pour lequel une bonne connaissance des nombres premiers jumeaux est un atout.

Écrivez les nombres de 1 à 100, ou téléchargez sur la page Web du présent ouvrage le plateau de jeu de marelle (vous le trouverez sous son nom anglais : *prime hopscotch board*). Le premier joueur prend un jeton et le place sur un nombre premier, qui est au maximum à cinq cases de la première case. Le second joueur prend le jeton et le déplace vers un nombre premier plus grand encore, à cinq cases maximum de là où le jeton se trouvait initialement. Le premier joueur fait de même, déplaçant le jeton sur une case contenant un nombre premier toujours plus grand, laquelle, une fois encore, doit être au maximum à cinq cases de là. Le perdant est le premier joueur incapable de déplacer son jeton selon les règles. Les règles sont : (1) le jeton ne peut pas être déplacé à plus de cinq cases de son point de départ ; (2) il doit toujours être déplacé vers une case contenant un nombre premier ; et (3) il ne peut pas être reculé ou laissé sur place.

● JOUEUR 1					● JOUEUR 2				
1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Fig. 1.21 Exemple d'une partie de la « marelle des nombres premiers » où chaque saut du jeton ne peut dépasser cinq cases.

La figure 1.21 illustre un scénario typique. Le joueur 1 a perdu car le jeton est sur le 23 et aucun nombre premier ne figure dans les cinq cases suivantes. Si le joueur 1 avait démarré la partie autrement, aurait-il connu un meilleur sort ? Si on regarde bien, on voit qu'une fois dépassée la case du 5, il n'y a pas beaucoup de possibilités. Celui qui place son jeton sur le 5 gagnera donc forcément, puisqu'il pourra, aux tours suivants, déplacer son jeton de la case 19 à la case 23, ne laissant à son adversaire aucun nombre premier où se placer par la suite. Le mouvement de départ est donc vital.

Mais qu'advient-il si nous modifions la règle du jeu ? Admettons qu'il soit désormais possible de se déplacer de sept cases maximum. Les joueurs peuvent désormais franchir le cap de la case 23, car le 29 est à six cases de là. Le mouvement d'ouverture a-t-il, dans le cas présent, une incidence ? Et sur quelle case la partie s'achèvera-t-elle ? Lorsqu'on joue une partie selon cette règle, on constate que le nombre de cases possibles est bien plus important, surtout lorsqu'il y a une paire de nombres premiers jumeaux.

Au premier coup d'œil, étant donné le grand nombre de possibilités, on se dit que l'ouverture importe peu. Or, en y regardant de plus près, on s'aperçoit que si on se retrouve sur le 89, on a perdu, car le prochain nombre premier est le 97, à huit cases de là. En analysant le début du jeu et en notant les nombres premiers situés avant le 89, on constate qu'il est essentiel de se retrouver à un moment ou un autre sur le 67, car ce n'est que de là

que l'on peut choisir de placer son jeton sur le 71 ou le 73. L'un de ces nombres premiers jumeaux permet de gagner la partie, l'autre entraîne tous les déplacements ultérieurs et conduit à perdre.

Le joueur qui se trouve sur le 67 peut donc remporter la partie, et il semblerait que le 89 ne soit pas si important. Mais comment faire pour être sûr d'atteindre cette case ? Si on regarde à nouveau en arrière, on s'aperçoit qu'une décision cruciale doit être prise par quiconque se trouve sur le nombre premier 37. De là, il est effectivement possible d'atteindre les nombres premiers jumeaux de mes filles, 41 et 43. Le joueur qui place son jeton sur le 41 est certain de remporter la partie. Donc, il semblerait que le vainqueur soit celui qui parvient à obliger son adversaire à placer le jeton sur la case 37. En continuant ce cheminement à rebours, on constate qu'il y a effectivement une ouverture gagnante. Si on place le jeton sur la case 5, on est sûr ensuite de pouvoir prendre toutes les décisions qui permettent d'accéder à la case 89 et donc à la victoire, car l'adversaire ne peut alors plus bouger, étant dans l'incapacité d'atteindre le nombre premier suivant.

Que se passe-t-il si nous continuons d'augmenter la longueur maximum de chaque saut ? Pouvons-nous être certains que la partie s'arrêtera toujours ? Admettons que le saut maximum soit de 99 cases — comment savoir si la partie ne va pas durer éternellement dès lors qu'il est possible de trouver un nombre premier parmi ces 99 cases ? Après tout, nous savons qu'il y a une infinité de nombres premiers, alors peut-être qu'à un certain moment on peut tout simplement sauter de nombre premier en nombre premier.

Il est possible de démontrer que la partie s'arrêtera toujours. Quelle que soit la taille du saut maximum, il y aura toujours une portion de nombres ne contenant aucun nombre premier plus grande que le saut maximum et, là, la partie sera terminée. Regardons comment trouver 99 nombres consécutifs dont aucun n'est un nombre premier. Prenez le nombre $100 \times 99 \times 98 \times 97 \times \dots \times 3 \times 2 \times 1$. Ce nombre s'appelle factorielle 100 et s'écrit « 100 ! ». Nous allons utiliser un fait évident concernant ce nombre : si vous prenez n'importe quel nombre entre 1 et 100, alors 100 ! est divisible par ce nombre.

Regardez la séquence de nombres consécutifs :

$$100 ! + 2, 100 ! + 3, 100 ! + 4, \dots, 100 ! + 98, 100 ! + 99, \\ 100 ! + 100$$

$100! + 2$ n'est pas un nombre premier car il est divisible par 2. De la même manière, $100! + 3$ n'est pas un nombre premier car il est divisible par 3. ($100!$ est divisible par 3, si on ajoute 3, il le demeure.) Aucun de ces chiffres n'est un nombre premier. Prenez $100! + 53$, qui n'est pas non plus un nombre premier car $100!$ est divisible par 53, et si nous ajoutons 53 le résultat demeure divisible par 53. Voici donc 99 nombres consécutifs dont aucun n'est un nombre premier. Si nous avons commencé à $100! + 2$ et non à $100! + 1$, c'est que cette méthode ne marche pas pour $100! + 1$ (qui d'ailleurs n'est pas un nombre premier non plus).

Ce site Web donne des informations sur le moment où la partie prend fin selon la taille des sauts :

<http://bit.ly/Primehopscotch>

Donc nous sommes sûrs que si le saut maximum est de 99 cases, notre partie de marelle de nombres premiers prendra fin à un moment donné. Mais $100!$ est un nombre extraordinairement grand. En réalité, la partie s'est achevée bien avant qu'on n'en arrive là : le premier endroit où un nombre premier est suivi de 99 nombres non premiers est la case 396 733.

Une chose est certaine, jouer à ce jeu révèle la nature erratique des nombres premiers parmi tous les nombres. Il n'y a aucun moyen de savoir où se trouve le nombre premier suivant. Mais pouvons-nous au moins trouver une formule astucieuse pour fabriquer des nombres premiers ?

LES LAPINS ET LES TOURNESOLS PEUVENT-ILS AIDER À TROUVER DES NOMBRES PREMIERS ?

Regardez les pétales d'un tournesol. Il y en a souvent 89, un nombre premier. Le nombre de paires de lapins après 11 générations est également 89. Les lapins et les tournesols auraient-ils une formule secrète pour trouver des nombres premiers ? Pas vraiment. Ils aiment le 89 pas parce qu'il s'agit d'un nombre premier, mais parce que c'est un des nombres préférés de la nature

— les nombres de Fibonacci. C'est en 1202 que le mathématicien italien Fibonacci a découvert cette importante suite de nombres alors qu'il tentait de comprendre la manière dont les lapins se multiplient (au sens biologique, et non mathématique).

Pour commencer, Fibonacci imagina une paire de bébés lapins, composée d'un mâle et d'une femelle. Appelons ce point de départ le mois 1. Dès le mois 2, ces lapereaux sont devenus des adultes capables de se reproduire. Ils donnent naissance au mois 3 à une nouvelle paire de lapereaux. (Pour cette expérience de pensée, nous partons du principe que toutes les portées sont composées d'un mâle et d'une femelle.) Au mois 4, la première paire d'adultes donne le jour à une autre paire de lapereaux. Leur première paire de lapereaux a maintenant atteint l'âge adulte, donc il y a désormais deux paires de lapins adultes et une paire de lapereaux. Au mois 5, les deux paires adultes donnent chacune naissance à une paire de lapereaux. Les lapereaux du mois 4 sont désormais en âge de procréer.

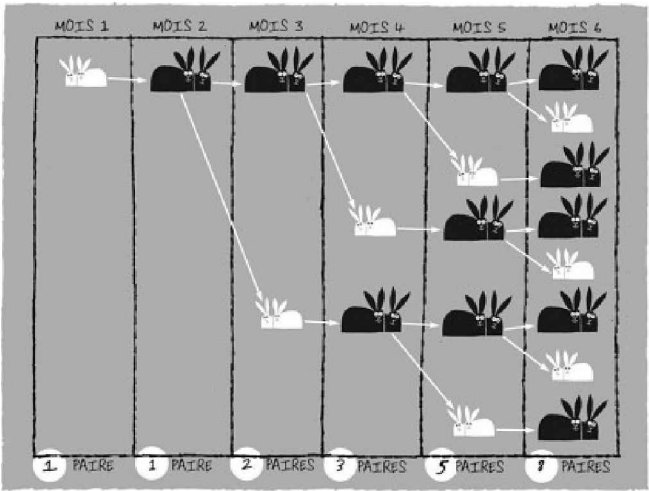


Fig. 1.22 Les nombres de Fibonacci donnent la croissance d'une population de lapins.

Donc, dès le mois 5, il y a trois paires de lapins adultes et deux paires de lapereaux, ce qui fait cinq paires de lapins au total. Le nombre de paires de lapins au fil des mois est donné par la suite :

1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89...

Tenir le compte de tous ces lapins qui se multipliaient... comme des lapins avait de quoi donner la migraine, mais Fibonacci trouva un moyen de calcul facile : pour obtenir le nombre suivant dans la suite, il suffit d'additionner les deux nombres précédents. Le plus grand des deux nombres est bien sûr le nombre de paires de lapins que l'on a à cet instant (on part du principe que tous survivent jusqu'au mois d'après), tandis que le plus petit de ces deux nombres est celui des paires adultes. Chacune de ces paires adultes engendre une autre paire de lapereaux et, le mois suivant, le nombre de lapereaux égale donc la somme des nombres représentant les deux précédentes générations.

Certains lecteurs reconnaîtront cette suite pour l'avoir déjà vue dans le roman de Dan Brown, *Da Vinci Code*. Cette suite est effectivement le premier code que le héros doit casser pour poursuivre sa quête du Saint-Graal.

Mais les lapins et Dan Brown ne sont pas les seuls à affectionner ces nombres. Les fleurs aussi ! Le nombre de pétales d'une fleur est souvent un nombre de Fibonacci. Le trillium en compte 3, la pensée 5, le delphinium 8, le souci 13, la chicorée 21, le pyrèthre 34 et les tournesols ont souvent 55 ou même jusqu'à 89 pétales. Certaines plantes ont un nombre de pétales qui est le double d'un des nombres de Fibonacci. Il s'agit de végétaux qui sont composés de deux « copies » d'une fleur, comme certains lys. Si votre fleur n'a pas un nombre de Fibonacci de pétales, c'est qu'elle en a sûrement perdu un... et voilà comment les mathématiciens se débrouillent avec les exceptions. (Ne souhaitant pas être inondé de courriers de jardiniers furieux, j'admets qu'il existe quelques exceptions qui n'ont rien à voir avec la fanaison des fleurs. La bourrache, par exemple, compte souvent sept pétales. La biologie n'est jamais aussi parfaite que les mathématiques.)

Les nombres de Fibonacci apparaissent aussi sur les pommes de pin et les ananas. Coupez une banane en deux et vous verrez qu'elle est divisée en trois segments. Coupez une pomme en deux à mi-distance entre la queue et la base et vous avez une étoile à cinq branches. Essayez avec un kaki et vous découvrirez une étoile à huit branches. Qu'il s'agisse de la population de lapins ou de la structure des végétaux, il semblerait que dès qu'il y a croissance les nombres de Fibonacci surgissent.

La manière dont les coquillages se développent fait aussi apparaître ces nombres. Un bébé escargot commence avec une minuscule coquille, en fait une petite maison carrée d'une seule pièce. Lorsque, en grandissant, sa coquille devient trop petite, il

ajoute une autre pièce à sa maison et répète le processus tandis qu'il continue de grandir. Comme il ne peut pas prendre appui sur grand-chose, la pièce qu'il ajoute a des dimensions forcément fondées sur celles des deux précédentes, tout comme les nombres de Fibonacci sont la somme des deux nombres précédents. Le résultat de cette croissance est une spirale dont la simplicité n'a d'égal que la beauté.

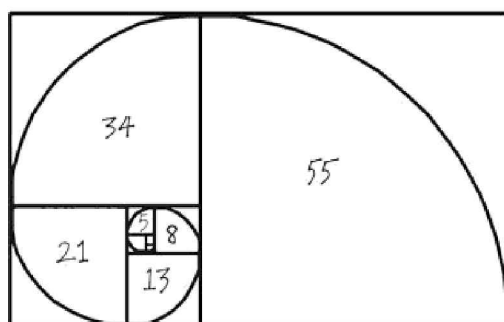


Fig. 1.23 Comment construire un coquillage à partir des nombres de Fibonacci.

En vérité, ces nombres ne devraient pas porter le nom de Fibonacci, car ce n'est pas lui qui les a découverts. En fait, ce n'est même pas un mathématicien qui les a révélés, mais des poètes et des musiciens dans l'Inde médiévale. Ces derniers cherchaient systématiquement toutes les structures rythmiques obtenues à partir de deux unités, courte et longue. Si un son long est deux fois plus long que le son court, alors combien de motifs différents sont possibles sur une longueur déterminée de battements ? Par exemple, avec huit battements on peut faire quatre sons longs ou huit sons courts. Mais entre ces deux extrêmes, les combinaisons sont nombreuses.

Au VIII^e siècle, l'écrivain indien Virahanka entreprit de déterminer le nombre exact de rythmes différents possibles. Il découvrit que lorsque le nombre de battements augmente, le nombre de motifs rythmiques possibles nous est donné par la suite suivante : 1, 2, 3, 5, 8, 13, 21... Il se rendit compte, comme Fibonacci quatre siècles plus tard, que pour arriver au nombre suivant dans la suite, il suffisait d'additionner les deux nombres précédents. Donc, si on veut savoir combien de rythmes sont possibles avec huit battements, on regarde le huitième nombre

dans la suite, qui a été obtenu en additionnant 13 et 21, et on obtient 34 motifs rythmiques différents.

Il est plus facile de comprendre le calcul du nombre de ces rythmes que de suivre la population des lapins de Fibonacci. Par exemple, pour obtenir le nombre de rythmes à base de huit battements, il suffit de prendre les rythmes de six battements et d'ajouter un son long ou bien de prendre les rythmes à sept battements et d'ajouter un son court.

Il existe un point commun très intéressant entre la suite de Fibonacci et les héros de ce chapitre, les nombres premiers. Prenons les premiers nombres de Fibonacci :

1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144...

Si p est un nombre premier, alors chaque p -ième nombre de Fibonacci est lui-même un nombre premier. Par exemple, 11 est un nombre premier et le 11^e nombre de Fibonacci est 89, un nombre premier. Si c'était toujours vrai, ce serait une formidable manière de trouver des nombres premiers toujours plus grands. Malheureusement, ce n'est pas le cas. Le 19^e nombre de Fibonacci est 4 181 et, bien que 19 soit un nombre premier, 4 181 ne l'est pas : il est égal à 37×113 . Aucun mathématicien n'a encore pu prouver s'il y a une infinité de nombres de Fibonacci qui soient premiers. C'est là un des nombreux mystères non résolus au sujet des nombres premiers.

COMMENT UTILISER DU RIZ ET UN ÉCHIQUIER POUR TROUVER DES NOMBRES PREMIERS ?

La légende dit que les échecs furent inventés en Inde par un mathématicien. Le roi était si reconnaissant envers le mathématicien qu'il lui demanda ce qu'il souhaitait recevoir comme récompense. L'inventeur réfléchit une minute, puis demanda qu'on place un grain de riz sur la première case de l'échiquier, deux grains sur la deuxième, quatre sur la troisième, huit sur la quatrième, et ainsi de suite, jusqu'à ce que chaque case contienne deux fois la quantité de riz de la case précédente.

Le roi accepta sur-le-champ, étonné que le mathématicien demande si peu — mais il n'était pas au bout de sa surprise. Au

début, les grains de riz étaient à peine visibles sur les cases. Puis, quand ils arrivèrent à la 16^e case, le roi fit venir un autre kilo de riz. À la 20^e case, c'est une brouette pleine de riz que ses serviteurs durent lui apporter. Jamais ils ne purent atteindre la 64^e et dernière case de l'échiquier. À ce stade-là, le nombre total de grains de riz sur l'échiquier aurait été hallucinant :

18 446 744 073 709 551 615

Si nous devons réitérer cet exploit dans le centre de Londres, par exemple, la pile de riz de la 64^e case s'étendrait jusqu'aux frontières du périphérique londonien, la M25, et serait si haute qu'elle recouvrirait tous les immeubles. En fait, il y aurait plus de riz dans cette pile que tout le riz produit dans le monde entier depuis mille ans.

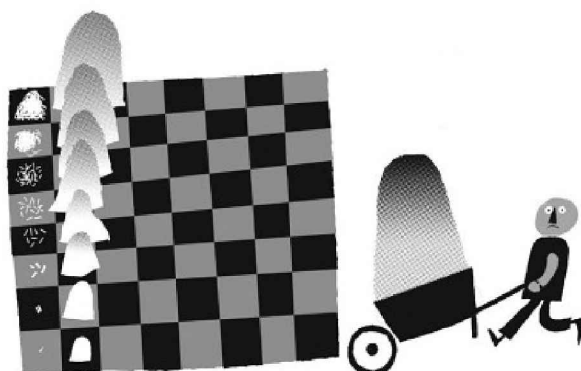


Fig. 1.24 Doubler une quantité de manière répétée fait grandir très vite les nombres.

Évidemment, le roi ne put donner satisfaction au mathématicien, et fut obligé de lui offrir la moitié de sa fortune. Ou comment devenir riche grâce aux mathématiques.

Mais quel est le lien entre tout ce riz et la recherche de grands nombres premiers ? Depuis que les Grecs ont prouvé que la suite des nombres premiers ne s'arrête jamais, les mathématiciens n'ont eu de cesse de chercher des formules astucieuses capables de produire des nombres premiers de plus en plus grands. Une des meilleures d'entre elles fut découverte par un moine français du nom de Marin Mersenne. Mersenne, qui était ami de Pierre de Fermat et de René Descartes, était à lui tout seul l'équivalent

XVII^e siècle d'une plateforme Internet car il recevait quantité de lettres des scientifiques de toute l'Europe et transmettait les idées qu'elles exposaient à ceux qu'il estimait pouvoir les exploiter.

Sa correspondance avec Fermat le conduisit à découvrir une puissante formule permettant d'identifier des nombres premiers immensément grands. Le secret de cette formule se cache dans la légende du riz et de l'échiquier. Lorsqu'on compte les grains de riz en partant de la première case de l'échiquier, bien souvent, l'addition donne un nombre premier. Par exemple, après trois cases, il y a $1 + 2 + 4 = 7$ grains de riz, un nombre premier. À la cinquième case, il y a $1 + 2 + 4 + 8 + 16 = 31$ grains de riz.

Mersenne se demanda si la somme des grains de riz d'une case portant un nombre premier et de toutes les cases précédentes donnait un résultat également premier. Si oui, cela permettrait de calculer des nombres premiers de plus en plus grands. Le principe consiste à choisir une case portant un nombre premier (la 7^e case, par exemple), puis à additionner tous les grains de riz des cases précédentes y compris ceux de la 7^e case. Mersenne espérait que le résultat de cette addition serait un nombre premier évidemment encore plus grand.

Malheureusement pour Mersenne et pour les mathématiques, son idée ne fonctionne pas. Si on prend par exemple la 11^e case de l'échiquier, un nombre premier, l'addition des grains de riz se trouvant sur les cases de 1 à 11 égale 2 047 grains de riz. Or, 2 047 n'est pas un nombre premier — il est égal à 23×89 . Si l'idée de Mersenne ne marche pas toujours, elle a néanmoins permis de découvrir certains des plus grands nombres premiers.

LE LIVRE GUINNESS DES NOMBRES PREMIERS

Sous le règne d'Élisabeth I^{re}, dans la seconde moitié du XVI^e siècle, le plus grand nombre premier connu était le nombre de grains de riz jusqu'à la 19^e case de l'échiquier comprise, soit 524 287 grains de riz. Au moment de la bataille de Trafalgar, en 1805, le record du plus grand nombre premier était toujours la 31^e case de l'échiquier : 2 147 483 647. Le mathématicien suisse Leonhard Euler a montré en 1772 que ce nombre à dix chiffres

était un nombre premier. Ce n'est qu'en 1867 que le record fut à nouveau battu.

Le 4 septembre 2006, le plus grand nombre premier connu était équivalent au nombre de grains de riz qui se seraient trouvés sur la 32 582 657^e case (il faudrait un très grand échiquier). Ce nouveau nombre premier a plus de 9,8 millions de chiffres, et il faudrait un mois et demi pour l'énoncer. Ce n'est pas un superordinateur qui est à l'origine de sa découverte, mais un mathématicien amateur aidé d'un logiciel qu'il a téléchargé sur Internet.

Le principe de ce logiciel est d'utiliser les périodes d'inactivité d'un ordinateur pour faire des calculs. Son programme met en œuvre une stratégie astucieuse pour vérifier la primalité des nombres de Mersenne. Bien qu'il ait fallu plusieurs mois pour que le PC passe en revue systématiquement les nombres de Mersenne à 9,8 millions de chiffres, cette méthode est bien plus rapide que celles consistant à tester de manière aléatoire des nombres de cette taille pour déterminer s'il s'agit de nombres premiers ou non. En 2009, plus de dix mille personnes avaient rejoint ce qui s'appelait désormais le projet GIMPS (Great Internet Mersenne Prime Search).

Cette recherche n'est cependant pas sans risque. Une des recrues du GIMPS, qui travaillait pour une compagnie de téléphone aux États-Unis, décida de mettre à contribution les 2 585 ordinateurs de sa société. Des employés commencèrent à soupçonner que quelque chose ne tournait pas rond lorsqu'ils s'aperçurent que les ordinateurs mettaient cinq minutes pour effectuer une tâche accomplie habituellement en cinq secondes.

Si vous souhaitez que votre ordinateur rejoigne le projet GIMPS, téléchargez le logiciel sur www.mersenne.org

Lorsque le FBI finit par trouver la cause du ralentissement, l'employé avoua : « C'était trop tentant, toute cette puissance informatique ! » La compagnie n'eut cependant aucune mansuétude pour ce travail de recherche et le malheureux fut renvoyé.

Après septembre 2006, les mathématiciens retenaient leur souffle : quand un nombre premier avec plus de 10 000 000 de chiffres serait-il trouvé ? Il faut préciser que la récompense n'était

pas seulement d'ordre académique, mais aussi financière, car 100 000 dollars attendaient la première personne capable de franchir ce cap. Ce prix était offert par l'Electronic Frontier Foundation, un organisme basé en Californie dont l'objectif est de promouvoir la collaboration internationale dans le cyberspace.

Encore deux ans et le record fut battu. Par un cruel caprice du destin, les deux nouveaux nombres premiers records furent trouvés à quelques jours d'intervalle. Le limier des nombres premiers, l'Allemand Hans-Michael Elverich, était persuadé d'avoir remporté le gros lot lorsque, le 6 septembre 2008, son ordinateur lui annonça qu'il venait de trouver un nouveau nombre premier de Mersenne composé de 11 185 272 chiffres. Mais lorsqu'il soumit sa découverte aux autorités, quelle ne fut pas sa déception : quelqu'un l'avait devancé de quatorze jours. En effet, le 23 août 2008, l'ordinateur d'Edson Smith au département de mathématiques de l'université de Californie à Los Angeles (UCLA) avait quant à lui découvert un nombre premier encore plus grand, long de 12 978 199 chiffres. Pour l'UCLA, battre des records de nombres premiers n'est pas une nouveauté. Le mathématicien Raphael Robinson y avait découvert cinq nombres premiers de Mersenne dans les années 1950, et Alex Hurwitz deux autres au début de la décennie suivante.

Les développeurs du programme utilisé par GIMPS estimèrent que la récompense devait être partagée et non remise dans sa totalité à celui qui avait eu la chance de se voir attribuer ce nombre premier de Mersenne, afin d'en vérifier la primalité. Ainsi, 5 000 dollars furent donnés aux développeurs du logiciel, 20 000 dollars furent partagés entre ceux qui avaient battu des records grâce à ce logiciel depuis 1999, 25 000 dollars donnés à une association caritative et le reste alla à Edson Smith en Californie.

Si l'idée de gagner de l'argent en cherchant des nombres premiers vous tente toujours, ne soyez pas découragé à l'idée que la barre des 10 000 000 de chiffres ait été franchie. Pour chaque nouveau nombre premier de Mersenne dont la primalité serait avérée, une récompense de 3 000 dollars sera attribuée. Mais si vous voyez plus grand, sachez qu'une récompense de 150 000 dollars vous attend si vous parvenez à franchir la barre des 100 millions de chiffres et 200 000 dollars si vous franchissez le cap du milliard. Grâce aux Grecs anciens, nous savons que de tels nombres premiers records existent et attendent quelque part dans le monde des nombres premiers que quelqu'un vienne les chercher.

Il faut plutôt se demander si l'inflation n'aura pas trop rongé le montant de ces prix quand ils seront attribués.

COMMENT ÉCRIRE UN NOMBRE DE 12 978 189 CHIFFRES

Le nombre premier trouvé par Edson Smith est d'une grandeur phénoménale. Il faudrait plus de 3 000 pages de ce livre pour transcrire l'ensemble des chiffres qui le composent ; heureusement, avec un peu d'arithmétique, il est possible de proposer une formule qui exprime ce nombre d'une manière bien plus succincte.

Le nombre total de grains de riz jusqu'à la N -ième case de l'échiquier est :

$$R = 1 + 2 + 4 + 8 + \dots + 2^{N-2} + 2^{N-1}$$

Voici une formule qui exprime simplement ce nombre. Au premier regard, on pense qu'elle sera inopérante tant elle est évidente : $R = 2R - R$. Comment croire un instant qu'une telle équation puisse nous aider à calculer R ? Dans le domaine des mathématiques, il est parfois utile d'adopter une perspective légèrement différente, tout peut alors soudain apparaître sous un nouveau jour.

Commençons par calculer $2R$. Cela signifie simplement doubler tous les termes dans la grande somme. Or, justement, si vous doublez le nombre de grains de riz dans une case, le résultat est le même que le nombre de grains de riz dans la case suivante. Donc :

$$2R = 2 + 4 + 8 + 16 + \dots + 2^{N-1} + 2^N$$

La prochaine étape consiste à soustraire R . Cela éliminera tous les termes de $2R$ à l'exception du dernier :

$$\begin{aligned} R &= 2R - R = (2 + 4 + 8 + 16 + \dots + 2^{N-1} + 2^N) - (1 + 2 + 4 + \\ &\quad 8 + \dots + 2^{N-2} + 2^{N-1}) \\ &= (2 + 4 + 8 + 16 + \dots + 2^{N-1}) + 2^N - 1 - (2 + 4 + 8 + \dots + 2^{N-2} + 2^{N-1}) \\ &= 2^N - 1 \end{aligned}$$

Donc le nombre total de grains de riz sur la N -ième case de l'échiquier est $2^N - 1$, et c'est à cette formule que l'on doit les nombres premiers records actuels. En doublant un nombre suffisamment de fois puis en soustrayant 1 de la réponse, vous pouvez peut-être espérer tomber sur un nombre de Mersenne premier (c'est ainsi que l'on appelle les nombres premiers trouvés grâce à cette formule). Pour obtenir le nombre premier à 12 978 189 chiffres trouvé par Edson Smith, il faut mettre $N = 43\,112\,609$ dans cette formule.

COMMENT TRAVERSER L'UNIVERS À L'AIDE D'UNE NOUILLE CHINOISE

Le riz n'est pas le seul aliment qui sert à comprendre le pouvoir du doublement pour créer de grands nombres. Les nouilles chinoises, et plus précisément les Lanzhou lamian, sont fabriquées de manière traditionnelle en étirant la pâte avec les bras et en la repliant sur elle-même pour doubler sa longueur. Chaque fois que l'on étire la pâte, la nouille devient plus longue et plus fine, mais il faut travailler vite car elle se dessèche rapidement.

Dans toute l'Asie, des cuisiniers tentent de relever le défi consistant à doubler la longueur de la nouille le plus de fois possible et, en 2001, le chef taïwanais Chang Hun-yu réussit à doubler sa pâte 14 fois en deux minutes. La nouille ainsi réalisée était si fine qu'elle pouvait passer par le chas d'une aiguille. Le pouvoir de doublement est tel que cette nouille aurait pu être étirée depuis le restaurant de M. Chang dans le centre de Taipei jusqu'à la périphérie de la ville ; et, quand finalement elle fut débitée, elle produisit 16 384 nouilles individuelles.

Voilà donc le pouvoir du doublement, et il peut très rapidement produire de très grands nombres. Par exemple, si Chang Hun-yu avait pu continuer de doubler sa nouille 46 fois, celle-ci aurait eu l'épaisseur d'un atome et une longueur allant de Taipei aux confins de notre système solaire. En doublant la nouille 90 fois, il serait possible de relier un côté de l'univers observable à l'autre. Pour entrevoir à quel point le nombre premier record actuel est grand, sachez qu'il faudrait doubler la nouille 43 112 609 fois puis soustraire une nouille. Le résultat : le nombre premier record découvert en 2008.

QUELLE EST LA PROBABILITÉ QUE VOTRE NUMÉRO DE TÉLÉPHONE SOIT UN NOMBRE PREMIER ?

Tout mathématicien qui se respecte cherche à savoir si son numéro de téléphone est un nombre premier. Récemment, après un déménagement, j'ai dû changer de numéro de téléphone. Mon numéro précédent n'était pas un nombre premier (en revanche, celui de la maison l'était, le 53), alors j'espérais vivement avoir plus

de chance cette fois-ci grâce à ma nouvelle demeure (située au n° 1 de la rue, nombre autrefois premier).

Le premier numéro qu'on m'attribua avait l'air prometteur, mais après l'avoir passé à la moulinette de mon ordinateur, j'ai vu qu'il pouvait être divisé par 7. « Je ne suis pas certain de pouvoir mémoriser ce numéro... Vous pourriez m'en donner un autre ? » Pas de chance non plus avec le numéro suivant : ce n'était pas un nombre premier puisqu'il était divisible par 3. (Voici une méthode simple pour déterminer si un nombre est divisible par 3 : additionnez par exemple tous les chiffres de votre numéro de téléphone, et si le nombre obtenu est divisible par 3, alors c'est également le cas du nombre de départ.) Après trois autres tentatives, mon interlocuteur, exaspéré, déclara d'un ton sec : « Monsieur, je suis navré mais je vais tout simplement vous attribuer le prochain numéro qui apparaît sur mon écran. » Hélas ! J'ai maintenant un numéro de téléphone pair, ce qui est pire que tout.

Quelle chance avais-je d'obtenir un numéro de téléphone qui soit un nombre premier ? Mon numéro comporte huit chiffres. Il y a approximativement 1 chance sur 17 qu'un nombre à huit chiffres soit un nombre premier, mais comment cette probabilité évolue-t-elle au fur et à mesure que le nombre de chiffres augmente ? Par exemple, il y a 25 nombres premiers inférieurs à 100, ce qui veut dire qu'un nombre composé d'au maximum deux chiffres a 1 chance sur 4 d'être un nombre premier. En moyenne, quand on compte de 1 à 100, on tombe sur un nombre premier tous les quatre nombres. Mais les nombres premiers se raréfient quand on va de plus en plus loin.

La table ci-dessous montre les différentes probabilités :

<i>Nombres de chiffres</i>	<i>Chance d'obtenir un nombre premier</i>
1 ou 2	1 chance sur 4
3	1 chance sur 6
4	1 chance sur 8,1
5	1 chance sur 10,4
6	1 chance sur 12,7
7	1 chance sur 15
8	1 chance sur 17,4
9	1 chance sur 19,7
10	1 chance sur 22

Table 1.02

Les nombres premiers deviennent de plus en plus rares, mais se raréfient de manière très régulière. Chaque fois que j'ajoute un chiffre, la probabilité décroît de manière presque identique — de 2,3 — à chaque fois. C'est un garçon âgé de quinze ans qui, le premier, se rendit compte de cela. Il s'appelait Carl Friedrich Gauss (1777-1855) et il allait devenir l'un des plus grands noms des mathématiques.

Gauss fit sa découverte après avoir reçu pour son anniversaire un livre de tables mathématiques qui se terminait par une table de nombres premiers. Il était tellement fasciné par ces nombres qu'il passa le reste de sa vie à ajouter d'autres nombres dans les tables à ses heures perdues. Gauss était un mathématicien expérimental qui aimait jouer avec des données et pensait que la manière dont les nombres premiers se raréfient se poursuivrait de façon uniforme aussi loin que l'on compte dans l'univers des nombres.

Mais comment être certain que quelque chose d'étrange ne va pas soudain survenir lorsqu'on atteint les nombres à 100 chiffres, ou à 1 million de chiffres ? La probabilité continuera-t-elle à décroître de 2,3 à chaque nouveau chiffre ? Ou va-t-elle, à un moment donné, commencer à se comporter de façon totalement différente ? Gauss pensait que ce motif récurrent (ou *pattern*) serait toujours là, mais il fallut attendre 1896 pour que d'autres en apportent la preuve formelle. Deux mathématiciens, Jacques

Hadamard et Charles de La Vallée Poussin, chacun de leur côté, apportèrent la preuve de ce qu'on appelle aujourd'hui le théorème des nombres premiers : les nombres premiers continueront toujours de se raréfier avec cette même régularité.

La découverte de Gauss a permis l'élaboration d'un modèle très puissant qui aide à prédire une grande partie du comportement des nombres premiers. C'est comme si, pour choisir les nombres premiers, la nature avait utilisé une série de dés spéciaux dont toutes les faces seraient vierges sauf une, qui porterait l'inscription NOMBRE PREMIER :

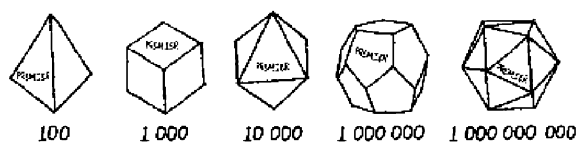


Fig. 1.25 Les dés de nombre premier de la nature.

Afin de décider si un nombre sera un nombre premier, on lance le dé. Si la face « nombre premier » sort, il est déclaré premier ; si c'est une face vierge, le nombre n'est pas déclaré premier. Bien sûr, il ne s'agit là que d'un modèle heuristique — on ne peut pas rendre 100 premier par un simple lancer de dé. Mais cela permet d'aboutir à une série de nombres dont la répartition est considérée comme très semblable à celle des nombres premiers. Le théorème des nombres premiers de Gauss nous dit combien de faces il y a sur un dé. Ainsi, pour des nombres à trois chiffres, il faut utiliser un dé à six faces ou un cube, dont une des faces porte la mention nombre premier. Pour des nombres à quatre chiffres, il faut un dé à huit faces. Pour un nombre à cinq chiffres, il faut un dé à 10,4 faces. Bien sûr, il s'agit là de dés théoriques car un polyèdre à 10,4 faces n'existe pas.

QU'EST-CE DONC QUE CE PROBLÈME DE NOMBRE PREMIER D'UNE VALEUR D'UN MILLION DE DOLLARS ?

La question à un million de dollars porte sur la nature de ces dés : sont-ils justes ou non ? Répartissent-ils justement, avec

régularité, les nombres premiers à travers l'univers des nombres, ou y a-t-il des régions où ils agissent de manière biaisée, distribuant parfois trop, parfois pas assez de nombres premiers ? Le nom de ce problème est l'hypothèse de Riemann.

Bernhard Riemann était un élève de Gauss à Göttingen, en Allemagne. Sa contribution aux mathématiques fut immense et grâce à certaines de ses découvertes nous comprenons désormais comment ce dé des nombres premiers répartit les nombres premiers. Riemann utilisa ce qu'on appelle la fonction zêta, des nombres nouveaux appelés nombres complexes et une dose impressionnante d'analyse pour comprendre les mathématiques qui contrôlent la chute de ces dés. Il était convaincu, d'après son analyse, que les dés seraient justes, mais sans pouvoir le prouver. Voici ce qu'il vous reste à faire : prouver l'hypothèse de Riemann.

Une autre manière d'interpréter l'hypothèse de Riemann consiste à comparer les nombres premiers à des molécules de gaz dans une pièce. Il est impossible de déterminer, à un instant donné, où se trouve chaque molécule, mais la physique nous dit que les molécules seront réparties de manière à peu près homogène dans la pièce. Il n'y aura pas un coin de la pièce avec une concentration de molécules et un autre avec un vide complet. L'hypothèse de Riemann aurait les mêmes implications pour les nombres premiers. Cela ne nous aide pas vraiment à déterminer où un nombre premier particulier se situe, mais cela garantit, en revanche, qu'ils sont répartis d'une manière homogène (bien qu'aléatoire) dans le monde des nombres. Ce genre de garantie est souvent suffisant pour permettre aux mathématiciens de naviguer dans l'univers des nombres en relative confiance. Cependant, tant que le million de dollars ne sera pas remporté, nous ne saurons jamais vraiment comment se comportent les nombres premiers tandis que nous traçons notre route toujours plus loin dans le cosmos sans limites des mathématiques.

Chapitre II

L'ÉTRANGE AFFAIRE DE LA FORME INSAISSABLE

Au XVII^e siècle, le grand savant Galilée écrivait :

[...] on ne peut [...] comprendre [l'Univers] si l'on ne s'applique d'abord à en comprendre la langue et en connaître les caractères avec lesquels il est écrit. Il est écrit en langue mathématique et ses caractères sont des triangles, des cercles et autres figures géométriques, sans le moyen desquels il est humainement impossible d'en comprendre un mot. Sans eux, c'est une errance vaine dans un labyrinthe obscur.

Ce chapitre présente l'ensemble des formes étranges et magnifiques de la nature : du flocon de neige à six branches à la spirale de l'ADN, de la symétrie radiale d'un diamant à la forme complexe d'une feuille. Pourquoi les bulles sont-elles parfaitement sphériques ? Comment le corps fabrique-t-il des formes aussi incroyablement complexes que le poumon humain ? Quelle est la forme de notre univers ? Les mathématiques sont essentielles pour comprendre comment et pourquoi la nature crée une telle diversité de formes ; non seulement elles nous donnent le pouvoir d'en créer des nouvelles, mais elles nous permettent de dire quand il n'y a plus d'autres formes à découvrir.

Les mathématiciens ne sont pas les seuls à s'intéresser aux formes : les architectes, les ingénieurs, les scientifiques et les artistes veulent tous comprendre comment fonctionnent les formes dans la nature. Pour cela, tous se fondent sur les mathématiques de la géométrie. Sur le fronton de son école, Platon avait fait graver la formule suivante : « Que nul n'entre ici s'il n'est géomètre. » Dans ce chapitre, je veux vous donner un laissez-passer pour l'univers de Platon, pour le monde mathématique des formes. Et dans les dernières pages de cette partie, je vous soumettrai une autre

énigme mathématique, dont la solution vaut, elle aussi, un million de dollars.

POURQUOI LES BULLES SONT-ELLES SPHÉRIQUES ?

Prenez un bout de fil de fer et tordez-le pour former un carré ; plongez cette forme dans un liquide à bulle et soufflez. Pourquoi la bulle qui se forme de l'autre côté n'est-elle pas carrée ? Pourquoi, quelle que soit la forme du cadre, la bulle sort toujours sous la forme d'une balle parfaitement sphérique ? Tout simplement parce que la nature est paresseuse et que la sphère est la forme la plus facile à obtenir. La bulle cherche la forme qui dépense le moins d'énergie, et cette énergie est proportionnelle à sa surface d'aire. La bulle contient un volume fixe d'air, et ce volume ne change pas si la forme change. La sphère est la forme qui a la plus petite surface d'aire pouvant contenir cette quantité fixe d'air, elle est donc celle qui utilise le moins d'énergie.

Les industriels cherchent depuis longtemps à imiter la manière dont la nature crée des sphères parfaites. Lorsqu'on fabrique des roulements à billes ou des balles pour des armes à feu, obtenir une sphère parfaite peut s'avérer une question de vie ou de mort, car une légère imperfection dans la forme sphérique peut provoquer l'explosion de l'arme ou le dysfonctionnement de la machine. En 1783, un plombier né à Bristol, William Watts, fit une découverte capitale en réalisant qu'il pouvait exploiter la préférence de la nature pour les sphères.

Lorsque du plomb fondu est lâché depuis le haut d'une tour, à l'instar de la bulle, les gouttelettes de liquide prennent la forme de sphères parfaites au cours de la chute. Watts se demanda si, en plaçant une cuve d'eau au pied de la tour, on pouvait figer les formes sphériques au moment où la gouttelette de plomb entrait en contact avec l'eau. Il décida de mettre son idée à l'épreuve dans sa maison de Bristol. Mais pour que le plomb fondu ait le temps de prendre la forme d'une sphère, il fallait que la goutte tombe d'une hauteur supérieure à trois étages.

Watts ajouta donc trois étages à sa maison et fit une découpe dans tous les sols afin de permettre une chute en ligne droite à travers le bâtiment. Les voisins furent plutôt surpris de l'apparition

soudaine d'une tour sur sa maison, à laquelle Watts s'efforça de donner une allure quelque peu gothique et ajouta un toit crénelé. Mais les expérimentations de Watts furent un tel succès que très vite des tours similaires furent construites un peu partout en Grande-Bretagne et aux États-Unis. La tour à plomb de Watts demeura en activité jusqu'en 1968.

Même si la nature utilise la sphère aussi souvent, comment être sûr qu'il n'existe pas une autre forme encore plus efficace que la sphère ? C'est le grand mathématicien grec Archimède qui, le premier, suggéra que la sphère était la forme ayant la plus petite surface d'aire pour un contenu de volume donné. Pour tenter de le prouver, Archimède commença par établir des formules pour calculer la surface d'aire d'une sphère et le volume qu'elle enferme.

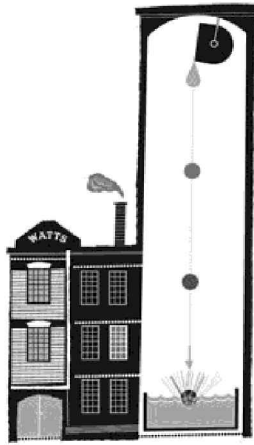


Fig. 2.01 L'utilisation astucieuse de la nature par William Watts pour fabriquer des roulements à billes sphériques.

Calculer le volume d'une forme courbe représentait un défi considérable, mais il eut recours à une astuce promise à un bel avenir : il découpa la sphère en une succession de disques parallèles de très faible épaisseur. Il connaissait déjà la formule pour calculer le volume d'un disque : c'était simplement l'aire du disque multipliée par son épaisseur. En additionnant les volumes de l'ensemble des disques composant la sphère, Archimède pouvait obtenir une approximation de son volume.



Fig. 2.02 Une sphère peut être reconstituée en empilant des disques de différentes tailles.

Mais s'il réalisait des disques infinitésimalement minces, la formule permettrait d'obtenir un calcul exact du volume. C'est l'une des premières fois que l'idée d'infini était utilisée en mathématiques. Près de deux mille ans plus tard, une technique similaire servira de base au calcul infinitésimal, une branche des mathématiques développée par Isaac Newton et Gottfried Leibniz.

Par la suite, Archimède utilisa cette méthode pour calculer les volumes de nombreuses autres formes. Il découvrit aussi qu'en plaçant une boule sphérique dans un cylindre de même hauteur, le volume d'air dans le cylindre est exactement la moitié du volume de la boule. Il en fut si fier qu'il demanda qu'une sphère inscrite dans un cylindre soit gravée sur sa tombe.

Bien qu'Archimède ait trouvé une méthode pour calculer le volume et la surface d'aire d'une sphère, il n'avait pas les moyens mathématiques indispensables pour démontrer son intuition qu'il s'agit là de la forme naturelle la plus économe en énergie. Étonnamment, ce n'est qu'en 1884 que les mathématiques atteignirent un niveau suffisamment avancé pour permettre à l'Allemand Hermann Schwarz de prouver qu'il n'existe aucune forme exigeant moins d'énergie que la sphère.

COMMENT FABRIQUER LE BALLON DE FOOT LE PLUS ROND DU MONDE

Beaucoup de sports se jouent avec des balles, des boules ou des ballons sphériques : le tennis, le cricket, le billard, le foot... Si la nature est douée pour fabriquer des sphères, les humains ont, eux,

plus de mal. Cela tient au fait que, la plupart du temps, nous fabriquons des balles ou des ballons en découpant des formes dans des feuilles planes d'un matériau quelconque, pour ensuite les mouler ou les coudre ensemble. Dans certains sports, on cherche justement à exploiter les imperfections de ces sphères. Une balle de cricket, par exemple, est constituée de quatre morceaux de cuir moulés et cousus ensemble, elle n'est donc pas véritablement sphérique. Un lanceur peut chercher à se servir de la couture proéminente pour faire rebondir la balle de manière imprévisible.

En comparaison, les pongistes exigent des balles parfaitement sphériques. Les balles de ping-pong sont fabriquées en collant ensemble deux hémisphères de celluloïd, mais la méthode laisse à désirer car plus de 95 % de la production est rejetée. Les fabricants de balles de ping-pong s'amuse comme des fous pour séparer les balles parfaitement sphériques des balles difformes : un pistolet propulse les balles en l'air et toutes celles qui ne sont pas sphériques iront à gauche ou à droite. Seules celles qui sont véritablement sphériques iront droit devant et seront collectées de l'autre côté du stand de tir.

Alors, comment fabriquer une sphère parfaite ? À l'approche de la Coupe du monde de football de 2006 en Allemagne, certains fabricants affirmèrent qu'ils étaient parvenus à créer le ballon le plus sphérique de tous les temps. La plupart des ballons de football sont fabriqués par l'assemblage de morceaux de cuir cousus ensemble, morceaux dont les formes remontent à l'Antiquité. Pour déterminer comment fabriquer le ballon de foot le plus symétrique possible, commençons par examiner les « balles » fabriquées à partir de plusieurs exemplaires d'un même morceau symétrique de cuir, agencés de manière que la forme solide ainsi assemblée soit elle aussi symétrique. Pour cela, on doit faire en sorte que le même nombre de faces se rencontrent à chaque sommet. Ces « balles », ce sont les solides présentés en 360 av. J.-C. par Platon dans son célèbre ouvrage le *Timée*.

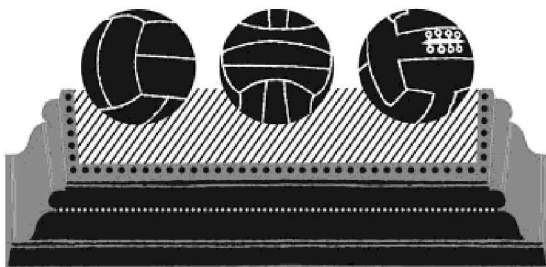


Fig. 2.03 Anciens modèles de ballons de foot.

À quoi ressemblent les différents ballons de foot selon Platon ? Celui qui requiert le moins d'éléments se compose de quatre triangles équilatéraux cousus ensemble pour former un tétraèdre — mais ce n'est pas un bon ballon de foot car il y a trop peu de faces. Comme nous le verrons au chapitre 3, cette forme n'a certes jamais été utilisée sur un terrain de foot mais elle a servi à d'autres jeux dans l'Antiquité.

Une autre possibilité est le cube, composé de six faces carrées. À première vue, cette forme semble trop stable pour un ballon, mais en réalité sa structure sous-tend beaucoup des premiers modèles du ballon de foot. Lors de la première édition de la Coupe du monde de football en 1930, un ballon fabriqué à partir de 12 bandes de cuir rectangulaires groupées en six paires et agencées en un cube fut utilisé. Bien que dégonflé et désormais asymétrique, un de ces ballons est aujourd'hui exposé au Musée national du football à Preston dans le nord de l'Angleterre. Un autre ballon assez extraordinaire, également utilisé dans les années 1930, est lui aussi monté en cube et se compose de six morceaux en H qui s'emboîtent astucieusement les uns dans les autres.

Mais revenons à nos triangles équilatéraux. Huit d'entre eux peuvent être agencés symétriquement pour donner un octaèdre, ce qui revient à faire fusionner deux pyramides à base carrée. Une fois fusionnées, il est impossible de savoir où se trouve la jointure.

Plus les solides de Platon possèdent de faces, plus ils vont sembler ronds. Après l'octaèdre, nous avons le dodécaèdre, dont les 12 faces sont pentagonales. Ce solide n'est pas sans lien avec les 12 mois de l'année, et plusieurs exemplaires datant de l'Antiquité ont été découverts, figurant des calendriers gravés sur les faces. Mais de tous les solides de Platon, c'est l'icosaèdre, composé de 20 triangles équilatéraux, qui s'approche le plus d'un ballon de foot sphérique.

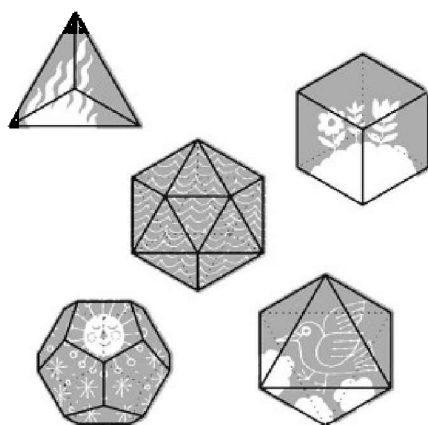


Fig. 2.04 Les solides de Platon étaient associés aux éléments, les blocs de construction de la nature. Selon Platon, ces cinq solides étaient fondamentaux au point qu'il les associa aux quatre éléments classiques, les « briques » de la nature : le tétraèdre, la plus pointue des formes, était associé au feu ; le cube, stable, à la terre ; l'octaèdre à l'air ; et la plus ronde des formes, l'icosaèdre, à l'eau. Platon estima que le cinquième solide, le dodécaèdre, représentait la forme de l'univers.

En vous rendant sur

www.4thestate.co.uk/2012/08/numbermysteries/, vous pouvez télécharger le fichier PDF contenant des instructions pour réaliser chacun des cinq ballons de foot de Platon. Fabriquez un but avec du bristol et testez l'efficacité des différentes formes en jouant au foot avec les doigts.

Comment être certain qu'il n'existe pas un sixième ballon de foot auquel Platon n'aurait pas songé ? C'est un autre mathématicien grec, Euclide, qui, dans un des plus grands ouvrages de mathématiques jamais écrits, apporta la preuve qu'il est impossible d'assembler une quelconque autre combinaison à base d'une unique forme régulière, et donc de fabriquer l'hypothétique sixième ballon de foot de Platon. Intitulé tout simplement *Éléments*, le livre d'Euclide est vraisemblablement à l'origine de la place fondamentale de la preuve logique en mathématiques. La force des mathématiques est de pouvoir apporter des certitudes à 100 %, et nous savons grâce à Euclide qu'il n'existe pas d'autres solides de ce type.

COMMENT ARCHIMÈDE A AMÉLIORÉ LES BALLONS DE FOOT DE PLATON

Et si on essayait d'arrondir certains des angles des cinq ballons de foot de Platon ? En prenant l'icosaèdre à 20 faces et en coupant toutes les pointes, on pourrait peut-être obtenir un ballon plus rond. Sur un icosaèdre, cinq triangles se rencontrent à chaque sommet, et si on tronque ces sommets, on obtient des pentagones. Les triangles dont les trois sommets ont été coupés deviennent alors des hexagones, et cet icosaèdre tronqué (c'est ainsi qu'il s'appelle) est en fait la forme du ballon de foot depuis la finale de la Coupe du monde de 1970 à Mexico. Mais existe-t-il d'autres solides créés à partir d'un assortiment de morceaux réguliers qui pourraient constituer un meilleur ballon pour la prochaine Coupe du monde ?

C'est au III^e siècle av. J.-C. que le mathématicien grec Archimède se mit à l'étude des solides de Platon. Il commença par assembler deux polygones différents (ou plus) pour composer les faces d'un solide. Pour que ces polygones puissent s'assembler parfaitement bord à bord, leurs côtés doivent être de même longueur. Pour obtenir le maximum de symétrie, il exigea aussi que la disposition en chaque sommet soit la même. Par exemple, si deux triangles et deux carrés se rejoignent en un des sommets, la même chose doit avoir lieu en tous les autres.

L'esprit d'Archimède était totalement absorbé par sa passion pour la géométrie. Même quand ses serviteurs arrachaient le savant à ses mathématiques pour le traîner malgré lui aux bains, il ne pouvait s'empêcher de dessiner des formes géométriques dans les cendres d'un feu ou dans les huiles parfumées dont son corps était enduit. Plutarque lui-même devait décrire comme « il était transporté hors de soi en extase du plaisir qu'il prenait à l'étude de la géométrie ».

C'est au cours de tels moments d'extase géométrique qu'Archimède conçut une classification complète des meilleures formes pour les ballons de foot, identifiant 13 différentes manières de les assembler. Le manuscrit dans lequel Archimède décrit ces formes n'a pas survécu ; cependant, grâce aux écrits de Pappus d'Alexandrie, qui vécut quelque cinq cents ans plus tard, nous possédons une trace de la découverte de ces 13 formes. Elles portent le nom de « solides d'Archimède ».

Archimède créa certains de ces solides en tronquant de petits morceaux des solides de Platon, comme ce fut le cas pour le ballon de foot classique. Par exemple, coupons les quatre pointes d'un tétraèdre. Les faces initialement triangulaires deviennent alors des hexagones, tandis que les faces produites par les coupes donnent quatre nouveaux triangles. Quatre hexagones et quatre triangles peuvent donc être assemblés pour produire une forme appelée tétraèdre tronqué (figure 2.05).

En fait, sept des 13 solides d'Archimède peuvent être créés en tronquant ainsi des solides platoniciens, dont le ballon de foot classique composé de pentagones et d'hexagones. Archimède a aussi découvert plusieurs autres formes plus remarquables encore. Par exemple, il est possible d'assembler 30 carrés, 20 hexagones et 12 polygones à dix faces (ou décagones) pour produire un polyèdre symétrique (figure 2.06) appelé grand rhombicosidodécaèdre convexe (ou aussi icosidodécaèdre tronqué).

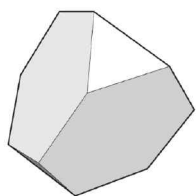


Fig. 2.05

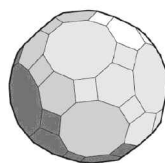


Fig. 2.06

C'est un de ces 13 solides d'Archimède qui inspira le nouveau ballon désormais en vogue ; utilisé pour la première fois lors de la Coupe du monde en Allemagne de 2006, il a été déclaré le ballon de foot le plus rond qui soit. Fabriqué à partir de 14 pièces courbes, ce ballon présente en réalité une structure fondée sur l'octaèdre tronqué, un solide composé de huit triangles équilatéraux dont on rase les six sommets. Les huit triangles deviennent des hexagones et les six sommets sont remplacés par des carrés (figure 2.07).

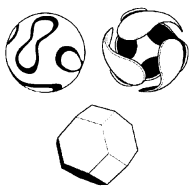


Fig. 2.07

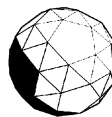


Fig. 2.08

Des images des 13 solides d'Archimède sont visibles à l'adresse suivante :

<http://bit.ly/Archimedean>

Peut-être qu'une des prochaines Coupes du monde se jouera avec un ballon inspiré d'un des solides plus exotiques encore d'Archimède. Si cela ne tenait qu'à moi, je choiserais le dodécaèdre adouci qui compte 92 faces, dont 12 pentagones et 80 triangles équilatéraux (figure 2.08).

Toute sa vie, Archimède se consacra avec passion aux mathématiques. Lorsqu'en 212 av. J.-C. les Romains envahirent Syracuse, il était tellement absorbé par une figure de géométrie qu'il ne se rendit même pas compte que sa cité était tombée aux mains de l'ennemi. Quand un soldat surgit dans sa maison, Archimède le supplia d'attendre un moment : « Laissez-moi finir ma démonstration ! » Mais le soldat n'avait que faire de sa démonstration et le transperça de son épée alors qu'il achevait son théorème.

QUELLE FORME DE THÉ PRENDREZ-VOUS ?

L'étude des formes est devenue un sujet brûlant non seulement pour les fabricants de ballons de foot mais aussi pour les buveurs de thé en Angleterre. Alors que nous nous sommes contentés pendant des années du simple sachet carré, voici que des cercles, des sphères et même des pyramides nagent désormais dans nos tasses !

Le sachet de thé a été inventé fortuitement, au début du xx^e siècle, par un marchand de thé new-yorkais du nom de Thomas Sullivan. Il avait envoyé à plusieurs de ses clients des échantillons de thé dans de petites aumônières de soie mais, au lieu d'enlever le thé de son emballage, les clients partirent du principe qu'ils devaient arroser le tout. Il fallut attendre les années 1950 pour que les Anglais adoptent enfin ce changement radical, et on estime aujourd'hui à plus de 100 millions le nombre de sachets de thé infusés chaque jour au Royaume-Uni.

Depuis des années, grâce à ce fidèle petit sachet carré, les amateurs de thé peuvent se préparer leur boisson préférée sans avoir à récurer la théière et retirer la myriade de feuilles restées collées aux parois. Le carré est une forme très économique — la fabrication de sachets de thé carrés est simple et facile, et ne gaspille pas de matériau puisque toute la surface est utilisée. Pendant un demi-siècle, PG Tips, le principal fabricant de sachets de thé, produisit ainsi des milliards de sachets chaque année dans des usines situées aux quatre coins du pays.

Mais en 1989, leur principal concurrent, Tetley, eut une idée audacieuse pour s'emparer du marché : lancer le sachet de thé rond. Bien que le changement fût surtout d'ordre esthétique, cela fonctionna, et les ventes du sachet rond grimpèrent en flèche. Les responsables de PG Tips comprirent qu'il fallait aller encore plus loin s'ils voulaient conserver leur part de marché. Le cercle avait peut-être excité le chaland, mais ce n'était, après tout, qu'une forme plane, une forme bidimensionnelle... L'équipe de chez PG Tips décida alors de faire le grand saut dans la troisième dimension.

Les équipes de PG Tips savent que nous n'avons que très peu de patience lorsqu'il s'agit de préparer notre thé. En moyenne, le sachet ne passe que 20 secondes dans la tasse avant d'être retiré. Si on incise un sachet bidimensionnel après 20 secondes d'infusion, on constate que les feuilles de thé situées au milieu sont complètement sèches, car elles n'ont pas eu le temps d'entrer en contact avec l'eau. Les chercheurs de PG Tips eurent alors l'idée d'un sachet tridimensionnel qui, par sa forme, se comporterait comme une mini-théière en permettant à toutes les feuilles d'entrer en contact avec l'eau. Ils embauchèrent même un expert en thermofluides de l'Imperial College de l'université de Londres afin d'élaborer des modèles informatiques pour appuyer l'hypothèse selon laquelle la troisième dimension pouvait améliorer le goût du thé.

Puis vint l'étape du développement du produit : quelle forme

choisir ? Plusieurs formes de sachets tridimensionnels furent préparées pour être testées auprès d'un panel de consommateurs. PG testa des sachets cylindriques, des sachets semblables à des lanternes chinoises ainsi que des sphères parfaites. La sphère est séduisante car, comme toute bulle vous le dira, c'est la forme tridimensionnelle qui, pour un volume donné, demande le moins de matériau pour réaliser le sachet. Mais c'est une forme difficile à fabriquer, surtout si l'on part d'un aplat de mousseline — si un jour vous avez tenté d'emballer un ballon de foot dans du papier cadeau, vous comprendrez.

Comme il s'agissait d'élaborer une forme à partir d'une surface plane de matériel, il semblait logique de commencer par des formes tridimensionnelles présentant des faces planes, et PG Tips entreprit d'examiner les formes décrites par Platon et Archimède il y a plus de deux mille ans. Les fabricants d'équipement sportif ont compris qu'un ballon composé de pentagones et d'hexagones est ce qui se rapproche le mieux d'une sphère, or c'est la forme située à l'autre bout du spectre qui commençait à intéresser les développeurs de sachets de thé. Bien que le tétraèdre à quatre faces, ou pyramide à base triangulaire, soit le polyèdre qui contient, pour une surface d'aire donnée, le moins de volume, il présente en revanche l'avantage d'avoir, de toutes les formes tridimensionnelles, le plus petit nombre de faces planes, ce qui facilite sa fabrication (il est en effet impossible de fabriquer une forme tridimensionnelle avec trois faces planes).

PG Tips souhaitait évidemment limiter au maximum le gaspillage du matériau servant à la confection des sachets, la forme devait donc être économique tout en demeurant visuellement attrayante. De plus, comme la marque désirait répondre à une demande de plus de 100 millions de tasses de thé par jour, il fallait que la forme choisie puisse être produite à haut débit : pas question d'avoir des usines remplies d'ouvriers en train de coudre ensemble quatre petits triangles pour confectionner des pyramides. Quelqu'un découvrit finalement une manière belle et élégante de fabriquer un sachet de thé en forme de pyramide.

Pensez à la façon dont se présente un paquet de chips. Un tube cylindrique de papier spécial est scellé en bas, rempli de chips puis scellé dans le même sens en haut. Regardez maintenant ce qui arrive si, au lieu de sceller le haut dans le même sens que le bas, vous tournez le paquet à 90° et scellez ensuite la partie supérieure. Vous tenez entre vos mains un paquet tétraédrique. Le tétraèdre a six arêtes : deux où les joints ont été faits, et quatre reliant les deux

joints (une arête court de l'extrémité de chaque joint jusqu'à chaque extrémité du joint opposé). Si on remplace le paquet de chips par un sachet de thé scellé, après cette même rotation, on obtient un sachet de thé pyramidal. Pas de gaspillage de matière, et une machine peut débiter ces sachets à un rythme de 2 000 par minute — vitesse suffisante pour satisfaire les besoins de la nation. Cette machine fut tellement innovante qu'elle est encore parmi les 100 meilleurs brevets déposés au XX^e siècle.

Après quatre ans de développement, le sachet de thé pyramidal fut lancé en 1996. Les consommateurs trouvèrent que la forme avait un aspect moderne et branché. La nouvelle campagne publicitaire apporta un heureux changement à la troupe de chimpanzés en habits utilisés pendant des années par le fabricant pour vendre son thé, et PG Tips regagna sa position de leader sur le marché du sachet de thé. Mais si les tétraèdres ont su faire ressortir le goût du thé, un autre des solides de Platon a quant à lui une saveur bien plus sinistre.

POURQUOI ATTRAPER UN ICOSAÈDRE PEUT-IL VOUS ÊTRE FATAL ?

En 1918, la pandémie de grippe espagnole fit au moins 50 millions de morts, bien plus que la Première Guerre mondiale. Face à une telle dévastation, les scientifiques s'acharnèrent à comprendre le mécanisme de cette dangereuse maladie et découvrirent rapidement que ce n'était pas une bactérie qui en était la cause mais quelque chose de bien plus petit et impossible à voir avec les microscopes de l'époque. Ils baptisèrent ces agents d'un genre nouveau, « virus », d'après le mot latin qui signifie poison.

Pour révéler la vraie nature de ces virus, il fallut attendre l'apparition d'une nouvelle technologie appelée la diffraction des rayons X, une méthode qui permet aux scientifiques de voir la structure moléculaire sous-jacente des organismes responsables de tels dégâts. Afin de visualiser une molécule, il n'est pas inhabituel d'utiliser des balles de ping-pong reliées entre elles par des cure-dents. Bien que cela semble un peu simpliste pour être scientifique, tous les labos de chimie possèdent de tels kits pour aider les étudiants et les chercheurs à modéliser les molécules. Lors de la diffraction des rayons X, un faisceau de rayons X est projeté à

travers l'objet examiné et les rayons X seront déviés, selon des angles différents, par les molécules rencontrées. Les images que l'on obtient ainsi ressemblent en quelque sorte à l'ombre que projetterait un de ces modèles à base de balles de ping-pong et de baguettes, éclairé latéralement.

Les mathématiques furent un puissant allié dans cette bataille pour lever le voile sur les informations contenues dans ces ombres. L'exercice consiste à déterminer quelles formes tridimensionnelles sont à l'origine des ombres bidimensionnelles produites par la diffraction des rayons X. L'angle de « l'éclairage » a son importance pour révéler au mieux les caractéristiques de la molécule. Par exemple, la silhouette en ombre chinoise d'une personne vue de face donne peu d'informations si ce n'est que les oreilles dépassent ; en revanche, un profil fournit bien plus d'informations sur la personne en question. Il en va de même avec les molécules.

Après avoir réussi à déchiffrer la structure de l'ADN, Francis Crick et James Watson, avec Donald Caspar et Aaron Klug, se concentrèrent sur ce que les images bidimensionnelles obtenues grâce à la diffraction des rayons X pouvaient révéler concernant les virus. À leur grande surprise, ils découvrirent des formes très symétriques. Les premières images montraient des points agencés en triangles, signifiant que le virus avait une forme tridimensionnelle qui, si elle subissait un tiers de tour, gardait la même apparence : signe de la présence d'une symétrie. Lorsque les biologistes regardèrent l'éventail des formes disposées sur les étagères des mathématiciens, ils comprirent que les solides platoniciens étaient ceux qui correspondaient le mieux à la forme de ces virus.

Mais les cinq solides platoniciens ont tous un axe à partir duquel il est possible de faire tourner la forme d'un tiers de tour afin que toutes les faces reprennent le même alignement. Ce n'est donc que lorsqu'ils eurent entre les mains une autre image par diffraction que les biologistes purent définir précisément les formes de ces virus. Sur cette nouvelle image, les points étaient disposés de manière à former un pentagone. Du coup, c'est vers l'un des solides platoniciens les plus intéressants que se dirigèrent les regards, l'icosaèdre, forme constituée de 20 triangles et de 12 sommets (où se rejoignent 5 triangles).

IMAGINER DES FORMES

Imaginez que vous accrochiez au sapin de Noël une décoration en forme de cube suspendue par un fil dépassant d'un des sommets. Si vous coupez le cube horizontalement à mi-distance entre la pointe du haut et la pointe du bas, vous obtenez deux morceaux, lesquels ont désormais chacun une face supplémentaire. Quelle est la forme de cette nouvelle face ? La réponse se trouve à la fin de ce chapitre.

Si les virus affectionnent les formes symétriques, c'est que la symétrie leur fournit une manière simple de se reproduire, et c'est pourquoi les maladies virales sont si infectieuses, *virulentes*, dira-t-on à juste titre. D'une manière générale, la symétrie provoque un plaisir esthétique chez les êtres humains, que ce soit celle d'un diamant, d'une fleur ou du visage d'un top model. Cependant, comme nous venons de le voir, la symétrie n'est pas toujours aussi souhaitable. Certains des pires virus, de la grippe à l'herpès en passant par ceux responsables de la polio ou du sida, sont construits à partir de la forme d'un icosaèdre.

LA PISCINE OLYMPIQUE DE PÉKIN EST-ELLE STABLE ?

Le bâtiment du Centre national de natation conçu pour abriter la piscine olympique des Jeux de Pékin est extrêmement beau, surtout la nuit lorsqu'il est éclairé et qu'il ressemble à une immense boîte transparente remplie de bulles. Ses concepteurs, le bureau Arup, souhaitaient à la fois exprimer l'esprit des sports aquatiques qui se dérouleraient à l'intérieur et produire une structure d'allure naturelle, organique.

Après avoir considéré des formes qui pourraient faire un carrelage sur le mur, c'est-à-dire des carrés, des triangles équilatéraux ou des hexagones, ils abandonnèrent l'idée car ces formes étaient jugées trop régulières, n'incarnant pas assez l'aspect organique de leur projet. Ils s'intéressèrent alors à la manière dont la nature organise des empilements, et examinèrent par exemple les cristaux et les structures cellulaires des végétaux. Dans toutes ces structures on retrouve des formes qu'Archimède avait identifiées comme faisant d'excellents ballons de foot, mais les

membres d'Arup furent surtout séduits par les formes qu'engendrent de nombreuses bulles compressées pour créer de la mousse.

Quand on sait que la preuve selon laquelle la sphère est la forme la plus économique pour *une* bulle ne fut apportée qu'en 1884, il n'y a rien d'étonnant à ce que les problèmes mathématiques liés à la formation de plus d'une bulle soient encore non résolus. Lorsque deux bulles contenant le même volume d'air fusionnent, quelle forme prennent-elles ? La règle est encore que les bulles sont paresseuses et cherchent à prendre la forme qui consomme le moins d'énergie. L'énergie étant proportionnelle à la surface d'aire, les bulles recherchent la forme ayant la plus petite surface d'aire de film de savon. Puisque deux bulles fusionnées partagent une frontière, elles peuvent créer une forme ayant une surface d'aire moindre que celle de deux bulles qui ne feraient que se toucher.

Si on souffle des bulles, et que deux bulles de même volume fusionnent, alors la combinaison a cette allure :

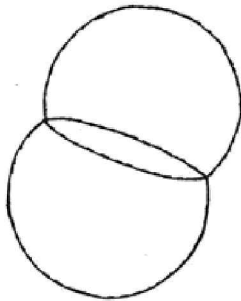


Fig. 2.09

Les deux sphères partielles se rencontreront à un angle de 120° et seront séparées par une paroi plane. On obtient certainement un état stable, sinon la nature ne laisserait pas les bulles sous cette forme. Mais existe-t-il une autre forme à la surface d'aire moindre, qui dépenserait donc encore moins d'énergie ? Pour sortir les bulles de leur état stable, il faudrait sans doute leur insuffler un peu d'énergie ; mais peut-être existe-t-il un état d'énergie plus faible. Par exemple, peut-être que les deux bulles pourraient être améliorées par une étrange configuration moins énergivore où une des bulles prendrait la forme d'un bagel qui viendrait entourer l'autre bulle pour lui donner la forme d'une coque de cacahuète (figure 2.10).

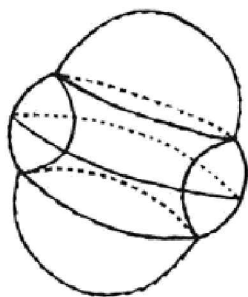


Fig. 2.10

La première preuve selon laquelle cette disposition est la meilleure fut apportée en 1995. Bien que les mathématiciens rechignent à se faire aider par l'outil informatique, estimant cela contraire à leur principe d'élégance et de beauté, ils durent cependant utiliser un ordinateur pour passer au crible les nombreux calculs numériques nécessaires.

Cinq ans plus tard, une preuve « manuelle » (c'est-à-dire sans aide informatique) de la conjecture de la double bulle fut annoncée. À vrai dire, elle prouvait aussi une conjecture plus générale : lorsque deux bulles ne contenant pas le même volume fusionnent, la paroi entre les deux bulles n'est plus plane et s'arrondit légèrement dans la plus grande des deux bulles. La preuve de la conjecture de la double bulle montrait désormais que cette paroi fait en réalité partie d'une troisième sphère qui sépare les deux autres bulles de manière à ce que les trois films de savon se rencontrent à des angles de 120° (figures 2.11 et 2.12).

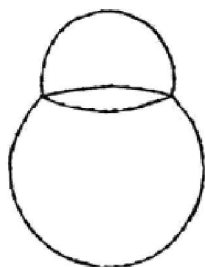


Fig. 2.11

En fait, cette propriété de 120° s'avère être une règle générale. C'est le scientifique belge Joseph Plateau, né en 1801, qui le

premier découvrit ce principe. Alors qu’il menait des recherches sur les effets de la lumière sur l’œil, il fixa le soleil pendant trente secondes et, à quarante ans, devint aveugle. Par la suite, aidé de sa famille et de collègues, il changea de sujet de recherche et se consacra à l’étude de la forme des bulles.

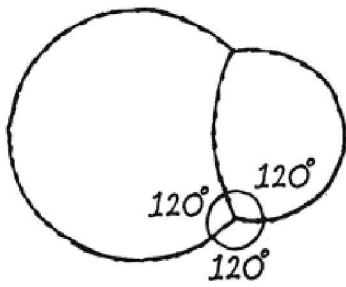


Fig. 2.12

Plateau commença par tremper des armatures en fil de fer dans du savon liquide afin d’examiner les différentes formes ainsi créées. Par exemple, lorsqu’on trempe une armature en fil de fer en forme de cube dans le mélange savonneux, on obtient 13 parois qui se rencontrent à l’endroit d’un carré situé au milieu (figure 2.13).

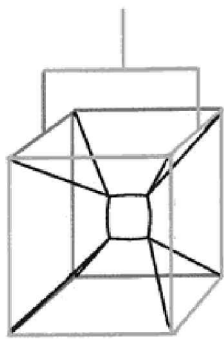


Fig. 2.13

Sauf que cette forme au milieu n’est pas vraiment un carré — les côtés sont comme bombés. Tandis que Plateau analysait les formes que faisaient émerger les différentes armatures, il commença à formuler une série de règles sur les surfaces d’aire de contact des bulles.

La première règle est que les films de savon se rencontrent toujours selon un angle de 120° . L'arête formée par ces trois parois s'appelle un bord de Plateau, en son honneur. La deuxième règle concerne la manière dont ces bords se rejoignent. Les bords de Plateau se rejoignent quatre par quatre à un angle de $109,47^\circ$ ($\cos^{-1} - 1/3$, pour être précis). Si on prend un tétraèdre et qu'on dessine des lignes reliant les quatre sommets vers le centre, on obtient la configuration des quatre bords de Plateau (figure 2.14). Donc, les arêtes du carré bombé au centre de l'armature en fil de fer se rencontrent en fait à $109,47^\circ$. Toute bulle ne correspondant pas aux règles de Plateau était instable et destinée par conséquent à s'effondrer en une configuration stable satisfaisant ces règles.

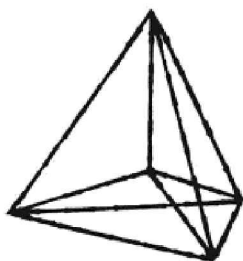


Fig. 2.14

Ce n'est qu'en 1976 que Jean Taylor apporta la preuve que la forme des bulles dans la mousse obéissait aux règles dictées par Plateau. Grâce au travail de cette chercheuse américaine, nous savons comment les bulles se connectent entre elles. Mais que savons-nous des *formes* que prennent les bulles dans la mousse ? Sachant que les bulles sont fainéantes, il faut, pour répondre à cette question, trouver les formes qui renferment une quantité d'air donnée dans chaque bulle de la mousse et qui, pour ce faire, utilisent une surface d'aire de film de savon aussi réduite que possible.

Les abeilles ont déjà trouvé la solution à ce problème en deux dimensions. Si elles construisent des ruches composées de cellules hexagonales, c'est qu'elles savent que l'hexagone est la forme qui nécessite le moins de cire pour contenir une quantité fixe de miel. Mais c'est à nouveau grâce à une découverte très récente que le théorème du nid d'abeille a pu être confirmé : nous savons désormais qu'il n'existe aucune autre structure bidimensionnelle

capable de surpasser la structure alvéolaire hexagonale en termes d'économie de matière.

Cependant, dès lors que nous passons à des structures tridimensionnelles, les choses deviennent moins évidentes. En 1887, le célèbre physicien britannique lord Kelvin émit l'idée qu'un des ballons de foot d'Archimède était la clé de la surface minimale des bulles. Il pensait que si l'hexagone était la brique de construction du nid d'abeille le plus économique, l'octaèdre tronqué — obtenu en rabotant les six sommets d'un octaèdre régulier — permettait la fabrication de la mousse :

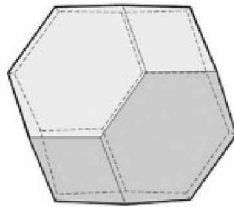


Fig. 2.15

Les règles développées par Plateau sur la manière dont les bulles de savon se recollent les unes aux autres affirment que les bords (ou arêtes) et les faces (ou parois) ne sont pas plans, mais courbes. Par exemple, les arêtes d'un carré se rencontrent à 90° , mais ce n'est pas permis par la deuxième règle de Plateau. Au lieu de cela, les arêtes du carré sont bombées, comme c'est le cas dans l'armature de fil de fer cubique, afin que les deux films de savon se rencontrent selon l'angle requis, c'est-à-dire $109,47^\circ$.

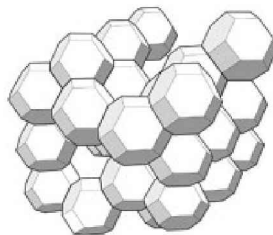


Fig. 2.16 Une mousse composée d'octaèdres tronqués.

Beaucoup de gens pensaient que la structure de Kelvin était le meilleur moyen de construire des bulles avec une surface d'aire

minimale, mais personne ne pouvait le démontrer. En 1993, cependant, Denis Weaire et Robert Phelan de l'université de Dublin identifièrent deux formes qui, assemblées, pouvaient battre la structure de Kelvin de 0,3 % (une mise en garde pour tous ceux qui pensent que prouver des choses en mathématiques est une perte de temps).

Il s'avère que les formes ne figurent pas sur la liste d'Archimède. La première est composée de pentagones irréguliers assemblés pour former un dodécaèdre tordu. La seconde forme s'appelle un tétrakaidécaèdre et se compose de deux faces hexagonales allongées et de 12 faces pentagonales irrégulières de deux genres différents. Weaire et Phelan ont réalisé qu'ils pouvaient entasser ces formes afin de créer une mousse encore plus « minimale » que celle proposée par Kelvin. Encore une fois, pour satisfaire aux règles de Plateau, les arêtes et les faces doivent être courbes et non droites. Comme il est plutôt difficile de pénétrer dans la mousse pour voir ce qui s'y passe réellement, ces formes furent découvertes grâce à des simulations numériques sur ordinateur.

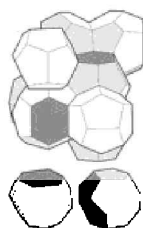


Fig. 2.17 Les formes découvertes par Denis Weaire et Robert Phelan.

Les bulles sont-elles capables de faire encore mieux ? Nous ne le savons pas. Nous pensons que c'est là le réseau le plus économique. Mais Kelvin aussi pensait avoir trouvé la réponse.

Les concepteurs d'Arup s'étaient intéressés au brouillard, aux icebergs et aux vagues dans leur quête de formes naturelles évocatrices de sports qui se dérouleraient à l'intérieur du centre de natation olympique. Lorsque, par hasard, ils tombèrent sur les mousses de Weaire et Phelan, ils réalisèrent qu'ils avaient sous les yeux un type de structure jamais tenté jusqu'alors dans le monde de l'architecture. Afin d'éviter de créer des formes trop régulières, ils décidèrent de scier la mousse en biais. Ce que vous voyez sur la façade du Cube d'eau, ou Water Cube (le surnom donné à ce centre

de natation), est en fait la forme des bulles après introduction en biais d'une plaque de verre dans la mousse.

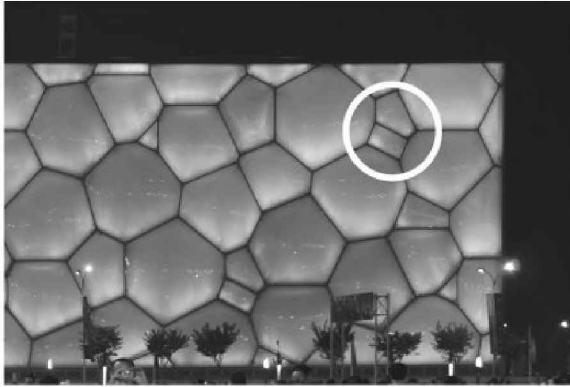


Fig. 2.18 Il semblerait que le centre olympique de natation de Pékin possède une bulle instable sur sa surface.

Bien que la structure conçue par Arup ait l'air aléatoire, en regardant de plus près, on voit que les éléments se répètent. Il n'empêche que l'ensemble parvient à donner l'impression organique voulue par les concepteurs. Et si on regarde d'encore plus près, on aperçoit une bulle qui ne semble pas répondre aux règles de Plateau car elle a des angles de 90° (alors que Plateau ne prévoit que des angles de 120° et $109,47^\circ$). Le Cube d'eau est-il stable ? S'il était vraiment fait de bulles, la réponse serait non. Cette bulle aux angles droits devrait changer sa forme pour satisfaire aux règles auxquelles toute bulle doit se soumettre. Cependant, les autorités chinoises n'ont pas de souci à se faire, le Cube d'eau a de grandes chances de rester debout, grâce notamment aux mathématiques qui sous-tendent la création de cette magnifique structure.

Arup et les autorités chinoises ne sont pas les seuls à s'intéresser à la forme que prennent des bulles qu'on comprime. La configuration de la mousse permet de comprendre la forme de nombreuses structures présentes dans la nature, non seulement celle des cellules dans les végétaux, mais aussi celle du chocolat, de la crème fouettée ou du chapeau de mousse d'une pinte de bière. On utilise la mousse pour éteindre un incendie, pour protéger l'eau d'une fuite radioactive et dans le traitement des minéraux. Comprendre la structure mathématique de la mousse est essentiel

dans bien des domaines, que ce soit pour maîtriser le feu ou expliquer pourquoi la mousse de votre Guinness tient si longtemps.

POURQUOI UN FLOCON DE NEIGE A-T-IL SIX BRANCHES ?

L'une des premières personnes à avoir tenté de répondre à cette question est Johannes Kepler, un astronome et mathématicien qui vécut au XVII^e siècle. En regardant l'intérieur d'une grenade, il comprit pourquoi les flocons de neige ont six branches. Au départ, les graines d'une grenade sont sphériques. Comme tout bon marchand d'oranges vous le dira, la manière la plus efficace d'empiler des balles sphériques consiste à les disposer en couches d'hexagones. Les strates se superposent ainsi de manière équilibrée, chaque balle confortablement nichée sur les trois balles de la couche en dessous. Ensemble, les quatre balles forment les sommets d'un tétraèdre.

Kepler émit la conjecture que c'était là le moyen le plus économique d'occuper l'espace — en d'autres termes, que cela correspond à un empilement où les espaces entre les balles, ou sphères, occupent un volume minimum. Mais comment être certain qu'il n'existe pas un autre agencement plus compact encore que celui en forme d'hexagone ? La conjecture de Kepler, car c'est ainsi que fut baptisée l'innocente affirmation, allait obséder plusieurs générations de mathématiciens. Une preuve ne fut apportée qu'à la fin du XX^e siècle, et pour cela les mathématiciens utilisèrent les moyens informatiques.

Revenons à notre grenade. Lorsque le fruit grandit, les graines commencent à être serrées les unes contre les autres, délaissant la forme sphérique pour des formes qui remplissent complètement l'espace. Chaque graine dans une grenade est en contact avec 12 autres graines, lesquelles, comprimées les unes contre les autres, prennent une forme à 12 faces. On pourrait penser qu'avec ses 12 faces pentagonales le dodécaèdre serait la forme adoptée par les graines, mais il n'est pas possible de compacter des dodécaèdres pour qu'ils remplissent totalement l'espace disponible. Le seul solide de Platon qui s'empile parfaitement pour remplir un espace est le cube. Au lieu de cela, les 12 faces de la graine dessinent une

forme en cerf-volant, le dodécaèdre rhombique, une forme fréquente dans la nature (figure 2.19).

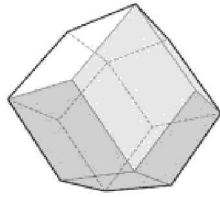


Fig. 2.19

Les cristaux de grenat ont 12 faces qui ressemblent à des cerfs-volants. Le mot « grenat » a la même origine latine que « grenade », car les graines du fruit forment également, comme nous venons de le voir, de petits solides rouges à 12 faces en forme de cerf-volant.

L'analyse des faces en forme de cerf-volant de la graine de grenade incita Kepler à rechercher toutes les formes symétriques possibles pouvant être construites à partir de cette face en cerf-volant légèrement moins symétrique. Platon avait étudié des formes faites à partir d'une seule face parfaitement symétrique ; Archimède était allé plus loin en examinant les formes composées d'au moins deux faces symétriques. Les recherches de Kepler déclenchèrent toute une série d'investigations consacrées à des formes différentes dans le prolongement des idées de Platon et d'Archimède. Aujourd'hui, nous avons les solides de Catalan, les solides de Poincaré, les solides de Johnson, des polyèdres flexibles et des zonoèdres — et bien d'autres objets exotiques.

Kepler estimait que l'agencement en hexagone comme moyen le plus efficace pour comprimer des sphères était également à l'origine des six branches d'un cristal de neige. Cette analyse fut le sujet d'un livre qu'il dédia à un diplomate impérial du nom de Matthaüs Wackher en guise de cadeau de nouvel an — geste perspicace de la part d'un scientifique en perpétuelle quête de mécénat. Lorsque des gouttelettes sphériques de pluie gèlent dans les nuages, pensait Kepler, elles s'entassent un peu comme les graines d'une grenade. Une jolie idée, mais qui se révéla fausse. La vraie raison des six branches du flocon est liée à la structure moléculaire de l'eau, phénomène que l'on ne comprit qu'avec l'invention de la cristallographie aux rayons X en 1912.

Une molécule d'eau se compose d'un atome d'oxygène et de deux atomes d'hydrogène. Lorsque des molécules d'eau

s'assemblent pour former des cristaux, chaque atome d'oxygène partage ses atomes d'hydrogène avec les atomes d'oxygène voisins, et emprunte deux autres atomes d'hydrogène à d'autres molécules d'eau. Ainsi, un cristal de glace n'apparaît que lorsque chaque atome d'oxygène est connecté à quatre atomes d'hydrogène. Une maquette composée de balles de ping-pong et de baguettes permet de visualiser la structure : imaginez quatre balles représentant les atomes d'hydrogène placées autour de chaque atome d'oxygène dans un agencement qui garantit que chaque atome d'hydrogène se trouve aussi loin que possible des trois autres atomes d'hydrogène. La solution mathématique à une telle exigence consiste à placer chaque atome d'hydrogène à un sommet d'un tétraèdre, le solide de Platon composé de quatre triangles équilatéraux, et de placer en son centre l'atome d'oxygène (figure 2.20).

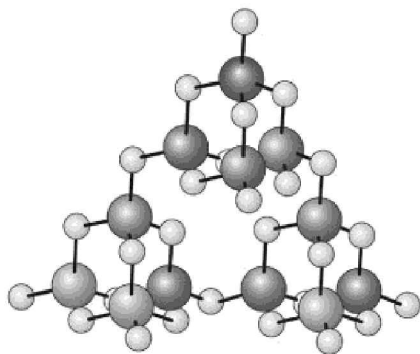


Fig. 2.20

La structure cristalline qui émerge n'est pas sans rappeler les piles d'oranges chez le primeur, où une orange est posée sur une strate composée de trois oranges, le tout formant un tétraèdre. Mais si on observe chaque strate d'oranges, on voit partout des hexagones. Ces hexagones, présents dans les cristaux de glace, sont la clé de la forme du flocon. Donc l'intuition de Kepler était juste : l'empilement d'oranges et le flocon ont bien quelque chose en commun, mais ce n'est que lorsqu'on put observer la structure atomique de la neige qu'il fut possible de déterminer où les hexagones étaient cachés. Quand le flocon de neige grandit, les molécules d'eau s'attachent aux six sommets de l'hexagone, ce qui fabrique petit à petit les six branches du flocon.

C'est lors de ce passage de la molécule au grand flocon que l'individualité de chaque flocon s'affirme. Et bien que la symétrie

soit au cœur de la création du cristal d'eau, c'est une autre forme mathématique importante qui régit l'évolution de chaque flocon : la fractale.

QUELLE EST LA LONGUEUR DU LITTORAL BRITANNIQUE ?

Le littoral de la Grande-Bretagne mesure-t-il 18 000 kilomètres de long ? 36 000 kilomètres ? Ou davantage encore ? Bizarrement, la réponse à cette question est loin d'être évidente, et elle est liée à une structure mathématique qui ne fut découverte qu'au milieu du XX^e siècle.

Bien sûr, avec les marées qui vont et viennent deux fois par jour, la longueur des côtes britanniques change sans cesse. Mais, même si nous décidons d'une hauteur de mer fixe, la longueur de la côte n'est toujours pas claire. Toute la difficulté réside dans le degré de précision voulu de la mesure. Nous pourrions commencer par placer des mètres de drapier bout à bout tout autour du pays, mais l'utilisation de ces règles rigides nous ferait rater beaucoup de petits détails.

En remplaçant le mètre de drapier par une longue corde, nous pourrions mieux épouser les formes complexes du littoral. Une fois la corde tendue et mesurée, nous obtiendrions une longueur de littoral considérablement supérieure à celle obtenue avec le mètre de drapier. Mais la flexibilité d'une corde a ses limites, et la corde non plus ne peut épouser tous les détails du littoral au centimètre près. Avec une ficelle, nous pourrions mieux suivre les contours, et alors notre estimation de la longueur de la côte serait encore plus élevée.



Fig. 2.21 Mesurer le littoral de la Grande-Bretagne.

Les géographes officiels ont déclaré que le littoral de la Grande-Bretagne mesure 17 819,88 kilomètres de long. Mais si nous le mesurons de manière plus détaillée, nous obtenons le double. Pour illustrer à quel point il est difficile d'arrêter les longueurs géographiques, sachez qu'en 1961 le Portugal annonça que sa frontière avec l'Espagne faisait 1 220 kilomètres de long, alors que l'Espagne disait qu'elle ne faisait que 990 kilomètres. Un écart de même ordre sépare les mesures néerlandaise et belge de leur frontière commune. En général, c'est toujours le pays le plus petit qui calcule la frontière la plus longue...

Ce processus connaît-il une limite ? Peut-être que plus nous regardons en détail, plus la côte devient longue ? Pour montrer pourquoi, construisons une section de côte mathématique. Pour tracer le littoral, vous aurez besoin d'une bobine de ficelle. Commencez par dérouler 1 mètre de ficelle que vous tendez sur le sol :



Fig. 2.22

Une vraie côte ne serait pas aussi droite, alors nous allons ménager un large bras de mer dans ce morceau de littoral. Débobinez un peu plus de ficelle afin de remplacer le tiers du milieu de votre ligne par deux côtés de même longueur, comme illustré ici :



Fig. 2.23

Combien de centimètres de ficelle avez-vous dû ajouter pour faire ce bras de mer ? La ligne avec laquelle nous avons commencé était composée de trois segments d'une longueur de $\frac{1}{3}$ m ; et cette nouvelle côte comprend quatre segments de $\frac{1}{3}$ m de long. La

nouvelle longueur est donc $\frac{4}{3}$ fois la première, c'est-à-dire $\frac{4}{3}$ m.

Mais cette nouvelle côte n'est toujours pas très accidentée. À nouveau, divisez chacun des segments en trois et remplacez le tiers du milieu de chaque segment par deux lignes de même longueur. Maintenant, nous obtenons cette côte :

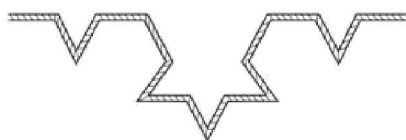


Fig. 2.24

Quelle est sa longueur ? Eh bien, chacun des quatre précédents segments est désormais plus long d'un facteur $\frac{4}{3}$. Donc la

longueur de la côte est maintenant $\frac{4}{3} \times \frac{4}{3}$ m = $(\frac{4}{3})^2$ m.

Vous avez sans doute deviné la suite. On répète le processus en divisant chaque ligne droite en trois et en remplaçant la portion du milieu par deux lignes de même longueur. À chaque fois, la longueur est multipliée par un facteur $\frac{4}{3}$. Si nous répétons

l'exercice 100 fois, la longueur de notre littoral sera multipliée d'un facteur $(\frac{4}{3})^{100}$, c'est-à-dire juste un peu plus de 3 milliards de kilomètres. Notre ficelle s'étirerait alors de la Terre à Saturne.

Si nous continuons ce processus, nous aurons une côte infiniment longue. Bien sûr, la physique nous empêche de diviser une chose au-delà d'une certaine limite, déterminée par ce qu'on appelle la constante de Planck. En effet, selon les physiciens, il est impossible de mesurer une distance plus petite que 10^{-34} m sans créer un trou noir qui avalerait l'appareil de mesure. Lorsque nous ajoutons des bras de mer de plus en plus petits à notre littoral, il faut s'imaginer qu'à la 72^e fois que nous procédons à cela, la longueur de chaque droite sera déjà inférieure à 10^{-34} m. Mais les mathématiciens ne sont pas des physiciens — nous, nous vivons

dans un monde où l'on peut diviser une droite infiniment de fois sans risquer pour autant de disparaître dans un trou noir.

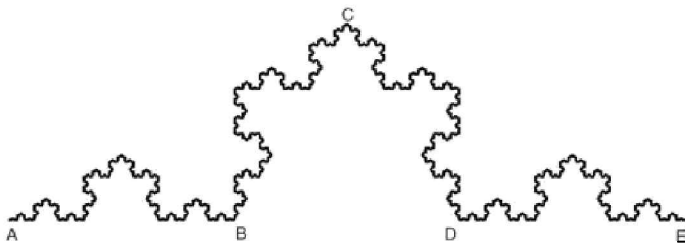


Fig. 2.25 En grossissant la section la plus petite, de A à B, par un facteur 3, on obtient une fractale plus grande. Mais la fractale plus grande peut aussi se construire en assemblant quatre copies de la section plus petite.

Une autre manière de comprendre pourquoi le littoral a une longueur infinie consiste à regarder de plus près la section de côte entre les points A et B dans le diagramme ci-dessus. Admettons que cette section soit de longueur L . Si nous grossissons ce morceau de côte trois fois, le résultat est une copie exacte de tout le littoral de A à E. Donc la totalité du littoral a une longueur de $3L$. D'un autre côté, si nous prenons quatre copies de cette section plus petite (toujours A à B), nous pouvons les mettre bout à bout pour couvrir la totalité du littoral : A à B, B à C, C à D et D à E. Dans ce cas, la longueur du littoral est $4L$, car nous avons besoin de quatre copies de la petite section (L) pour le construire. Or, quelle que soit notre façon de mesurer, notre côte a forcément une seule longueur ! Alors comment $4L$ peut-il être égal à $3L$? La seule manière de résoudre cette équation est si L est de longueur zéro ou de longueur infinie.

La côte infinie que nous avons dessinée est en fait un côté de la forme appelée flocon de Koch d'après le nom du mathématicien suédois Helge von Koch qui l'inventa au début du XX^e siècle (figure 2.26).

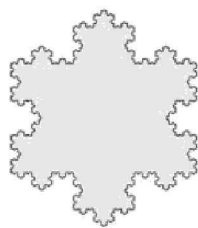


Fig. 2.26

Cette forme mathématique a trop de symétrie pour ressembler à un vrai littoral, et elle n'a pas l'air très naturelle ou organique ; en revanche, si on décide que les lignes qui forment les bras de mer sont parfois dirigées vers l'extérieur (comme de mini-isthmes) et ce, de manière aléatoire, alors l'ensemble devient bien plus convaincant. Voici des « images de côtes » (figure 2.27) réalisées selon le même procédé qu'auparavant, sauf que la décision de remplacer certaines lignes par un bras de mer ou au contraire par un isthme est tirée à pile ou face.

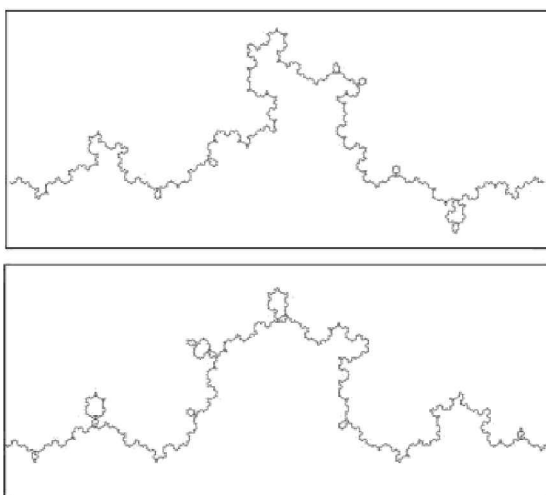


Fig. 2.27

En juxtaposant plusieurs de ces côtes, on obtient un tracé qui ressemble de manière étonnante à une carte médiévale du littoral britannique :

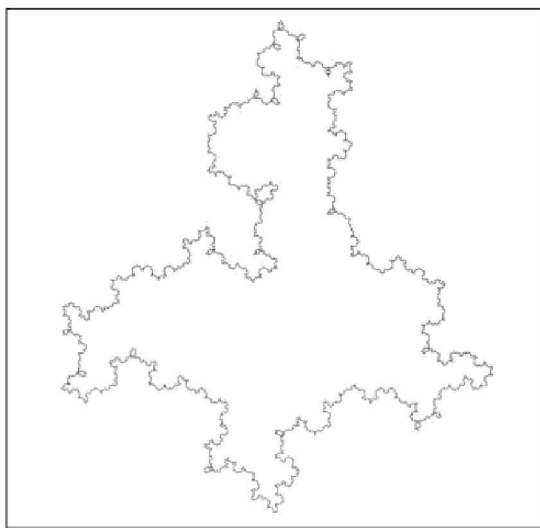


Fig. 2.28

Donc, si jamais on vous demande quelle est la longueur de la côte britannique, franchement, vous pouvez répondre ce que vous voulez. N'est-ce pas le genre de question de mathématiques qu'on aurait rêvé d'avoir à l'école ?

LES ÉCLAIRS, LES BROCOLIS ET LA BOURSE : QU'ONT-ILS EN COMMUN ?

En 1960, le département d'économie de l'université Harvard demanda au mathématicien français Benoît Mandelbrot de donner une conférence pour présenter ses derniers travaux sur la distribution des revenus. En entrant dans la salle de cours du professeur qui l'avait invité, il fut assez perturbé de voir les graphiques qu'il avait préparés pour son intervention déjà tracés sur le tableau noir. « Comment avez-vous fait pour vous procurer mes données ? » demanda-t-il. Or, chose incroyable, ces graphiques n'avaient rien à voir avec la répartition des revenus, ils décrivaient les variations du prix du coton en Bourse, le sujet du cours précédent.

Leur étonnante similarité piqua la curiosité de Mandelbrot qui, après avoir mené son enquête, put confirmer que des graphiques

représentant des séries de données économiques appartenant à des sujets ou à des domaines sans lien entre eux revêtent une forme semblable ; et ceci, quelle que soit l'échelle de temps choisie. Ainsi, les variations du prix du coton sur huit ans ressemblent aux variations sur huit semaines qui ressemblent à celles sur huit heures.

C'est ce même phénomène qui est à l'œuvre avec les côtes britanniques. Prenez, par exemple, les illustrations ci-contre. Toutes représentent une section de la côte de l'Écosse. Une des images reprend une carte à l'échelle 1/1 000 000. Les deux autres illustrations reprennent des cartes plus détaillées : une est à l'échelle 1/50 000, l'autre à l'échelle 1/25 000. Mais pouvez-vous deviner l'échelle de chacune ? Il semblerait que, quel que soit le degré de grossissement, les formes conservent le même degré de complexité. Cela n'est pas vrai de toutes les formes cependant ; si vous dessinez une ligne en zigzag et grossissez une section de ce dessin, à un moment donné, cela commencera à avoir l'air plus simple. Ce qui caractérise la forme d'un littoral ou les graphiques de Mandelbrot, c'est que, quel que soit le degré de grossissement, la complexité de la forme est conservée.

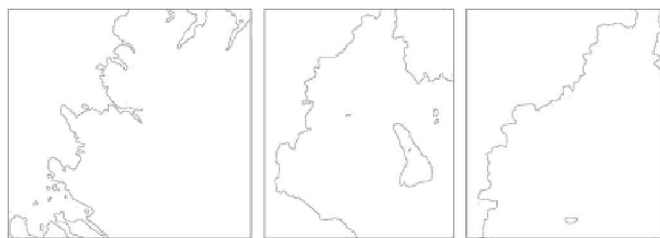


Fig. 2.29 Le littoral écossais selon différents degrés de grossissement. De gauche à droite : cartes dont l'échelle originelle est 1/1 000 000, 1/50 000 et 1/25 000.

Lorsque Mandelbrot élargit sa recherche vers d'autres champs d'investigation, il constata la présence de ces étranges formes — qui restent infiniment complexes à quelque niveau de grossissement que vous les regardiez — dans l'ensemble du monde naturel. Si l'on rompt une fleurette de chou-fleur et qu'on la grossit, elle ressemble étonnamment au chou-fleur entier. Si on grossit un éclair d'orage pour en extraire une portion, on s'aperçoit que cette section agrandie n'est absolument pas droite et ressemble à une copie de la totalité de l'éclair dont elle est issue. Mandelbrot donna

le nom de « fractales » à ces formes. Elles constituaient pour lui « la géométrie de la nature » car elles représentent une nouvelle sorte de forme mise au jour au XX^e siècle seulement.

Il existe une raison pratique à l'évolution naturelle de ces formes fractales. Le caractère fractal du poumon humain, par exemple, signifie que même s'il est logé dans le volume limité de la cage thoracique, sa surface d'aire est immense, et il peut donc absorber beaucoup d'oxygène. C'est également vrai pour d'autres objets organiques. La fougère cherche ainsi à maximiser son exposition à la lumière du soleil tout en s'efforçant de ne pas occuper trop de place. Nous avons à nouveau affaire à une nature capable d'identifier la forme la plus efficace possible. Tout comme la bulle a élu la sphère comme étant la forme la mieux adaptée à ses besoins, les formes vivantes ont cherché de l'autre côté du spectre et ont choisi des formes fractales d'une infinie complexité.

Il est remarquable de constater que, bien qu'infiniment complexes, les fractales sont engendrées par des règles mathématiques très simples. À première vue, il est difficile de croire que la complexité du monde naturel puisse être fondée sur des mathématiques simples, mais la théorie des fractales a permis de révéler que même les caractéristiques les plus complexes du monde naturel peuvent être le fait de formules mathématiques simples.

La figure 2.30 semble représenter une fougère, mais c'est en fait une image créée par ordinateur selon une règle mathématique analogue à celle utilisée pour concevoir le flocon de Koch. L'industrie informatique a su exploiter ce principe pour créer les décors compliqués de nombreux jeux vidéo. Même si une console de jeux repose sur un disque aux capacités limitées, une simple règle issue des mathématiques des fractales peut permettre de générer des décors complexes.



Fig. 2.30 Une fougère fractale.

COMMENT UNE FORME PEUT-ELLE AVOIR LA DIMENSION 1,26 ?

Avant l'entrée en scène des fractales, les formes rencontrées par les mathématiciens étaient uni-, bi- ou tridimensionnelles, une droite unidimensionnelle, un hexagone bidimensionnel, un cube tridimensionnel. Cependant, une des découvertes les plus étonnantes de la théorie des fractales est que ces formes d'un genre nouveau ont une dimension supérieure à 1 mais inférieure à 2. Comment une forme peut-elle avoir une dimension comprise entre 1 et 2 ? Vous êtes courageux ? Alors voici une explication.

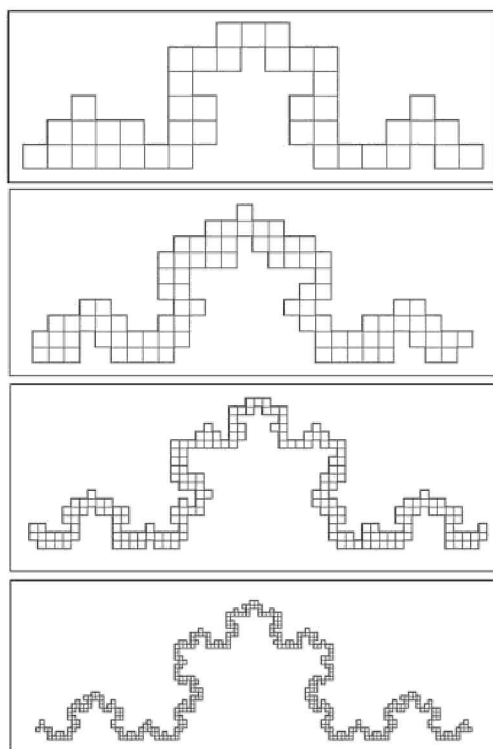


Fig. 2.31 Comment calculer la dimension d'une fractale avec du papier millimétré. La dimension mesure l'augmentation du nombre de pixels à mesure que l'on réduit la taille des pixels.

Le but est de trouver un moyen astucieux de comprendre pourquoi une droite est unidimensionnelle alors qu'un carré est bidimensionnel. Imaginez que vous prenez une feuille de papier-calque millimétré, que vous la posez sur une forme quelconque et que vous comptez combien de carreaux contiennent une partie de

la forme. Ensuite, prenez une feuille de calque millimétré dont les carreaux sont deux fois plus petits que ceux de la première feuille. Si la forme choisie est une droite, le nombre de carreaux sur le papier-calque augmentera d'un facteur 2. Si la forme est un carré plein, le nombre de carreaux augmente d'un facteur 4, ou 2^2 .

Chaque fois que nous réduisons de moitié la taille du quadrillage du papier-calque, le nombre de carreaux qui recouvrent une forme unidimensionnelle augmente de $2 = 2^1$, tandis que pour une forme bidimensionnelle, le nombre augmente de 2^2 . La dimension correspond à la puissance de 2.

Curieusement, si on applique ce procédé au littoral fractal construit plus tôt dans ce chapitre, lorsque nous réduisons de moitié la taille du quadrillage du papier millimétré, le nombre de carreaux contenant une partie de la côte augmente d'un facteur d'environ $2^{1,26}$. Nous avons donc donné une nouvelle définition de la dimension.

Pour reproduire ces formes, il est possible de remplacer le papier millimétré par un écran d'ordinateur pixélisé. Mettez en noir un pixel s'il contient un peu de la forme, sinon laissez-le blanc. Lorsque nous augmentons la résolution de l'écran, la dimension suit l'augmentation du nombre des pixels noirs qui apparaissent. Par exemple, si vous passez de 16×16 pixels à 32×32 , et que votre forme est une droite, alors le nombre de pixels noirs doublera. S'il s'agit d'un carré plein, le nombre de pixels noirs augmentera d'un facteur 4, ou 2^2 . En revanche, le nombre de pixels noirs d'un rendu informatique du flocon de Koch augmentera, lui, d'un facteur $2^{1,26}$.

D'une certaine manière, la dimension nous indique combien cette droite fractale infinie essaie de remplir l'espace qu'elle occupe. Si nous dessinons des variantes de notre littoral fractal où l'angle des bras de mer ou isthmes que nous ajoutons est à chaque variante plus petit, alors, au fur et à mesure, la ligne côtière remplit de plus en plus l'espace. Et lorsque nous calculons la dimension de chacune de ces variantes, nous voyons qu'elle se rapproche sans cesse davantage de 2 (figure 2.32).

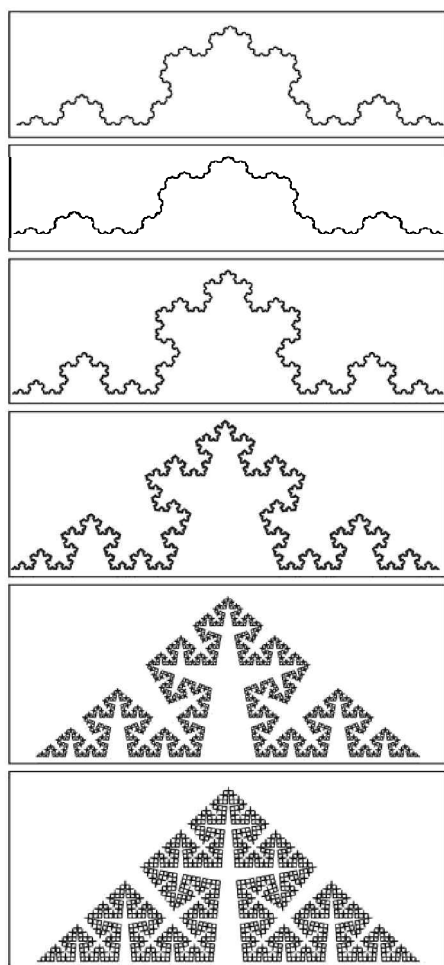


Fig. 2.32 En réduisant l'angle du triangle (forme par les deux lignes qui dessinent le bras de mer ou l'isthme), la fractale résultante occupe plus de place, et sa dimension fractale augmente.

L'analyse de la dimension fractale de formes qui se produisent naturellement fait apparaître des choses intéressantes. On estime la dimension fractale du littoral de la Grande-Bretagne à 1,25 — ce qui est très proche du littoral mathématique que nous avons construit. Nous pouvons envisager la dimension fractale comme une chose qui nous indique la vitesse à laquelle la longueur du littoral augmente tandis que les outils que nous utilisons pour mesurer la côte sont de plus en plus petits. La dimension fractale du littoral de l'Australie est estimée à 1,13, ce qui indique que, d'une certaine manière, la côte australienne est moins accidentée que le littoral britannique. La dimension fractale du littoral de l'Afrique du Sud est seulement 1,04, signe qu'il est très « lisse ». Le

littoral le plus fractal est sans doute celui de la Norvège, en raison de ses nombreux fjords — sa dimension fractale est 1,52.

Pour les objets tridimensionnels, il est possible de répéter le même exercice en remplaçant le papier millimétré par une sorte de grillage de cubes et en regardant comment la forme « recoupe » ces cubes tandis que le grillage gagne en finesse. Il en ressort que le chou-fleur est une forme de dimension 2,33, qu'une feuille de papier froissée en boule atteint 2,5, qu'un brocoli, dont la forme est très compliquée, arrive à 2,66, et que la surface du poumon humain a une dimension fractale de 2,97.

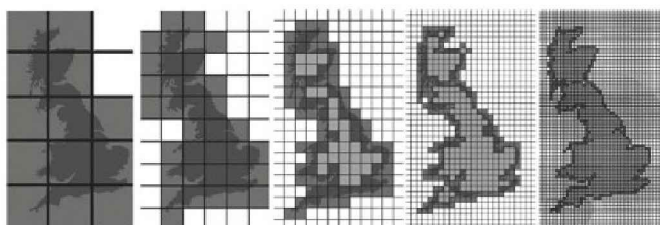


Fig. 2.33 Quelle est la dimension de la côte britannique ?

PEUT-ON FAIRE UN FAUX JACKSON POLLOCK ?

À l'automne 2006, le prix de vente d'une toile du célèbre expressionniste abstrait Jackson Pollock battit tous les records. La presse annonça qu'un financier mexicain du nom de David Martinez avait payé 140 millions de dollars pour ce tableau intitulé simplement *No. 5, 1948*.

Pour créer cette œuvre, Pollock avait eu recours à sa technique habituelle consistant à faire dégouliner ou à éclabousser de la peinture sur la toile. Certains critiques étaient choqués du prix atteint par un tel tableau, déclarant : « Eh bien, j'aurais très bien pu faire ça moi-même ! » et, à première vue, c'est vrai qu'on a l'impression que n'importe qui pourrait faire gicler de la peinture de la sorte et espérer faire fortune. Mais les mathématiques ont révélé que Pollock faisait quelque chose de bien plus subtil qu'on ne l'imaginait.

En 1999, un groupe de mathématiciens dirigé par Richard Taylor de l'université de l'Oregon analysa les peintures de Pollock

et découvrit que la technique saccadée qu'il utilisait crée en fait une des formes fractales tant appréciées par la nature. Lorsque des parties d'une toile de Pollock sont agrandies, elles continuent de ressembler étroitement à l'œuvre dans sa version à taille réelle et possèdent l'infinie complexité qui caractérise une fractale. (Bien sûr, à force de grossir un détail, on arrive aux touches de peinture elles-mêmes, mais seulement lorsque la toile est agrandie 1 000 fois.) La manière dont la technique de Pollock a évolué peut même être analysée à l'aune du concept de dimension fractale.

Pollock a commencé à créer des images fractales en 1943. Ses premières toiles présentent une dimension fractale aux alentours de 1,45, proche de la valeur des fjords de Norvège, mais à mesure qu'il met au point sa technique, la dimension fractale de ses peintures augmente, reflet de la complexité grandissante de ses toiles. Pollock devait consacrer six mois à la création d'une de ses dernières *drip paintings*, une peinture intitulée *Blue Poles* dont la dimension fractale est de 1,72.

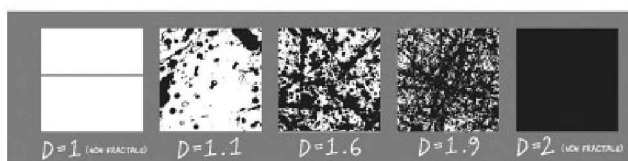


Fig. 2.34 La dimension fractale d'une peinture augmente à mesure que vous éclaboussez plus de peinture.

Les psychologues ont analysé les formes qui paraissent souvent belles. Il semblerait que nous soyons systématiquement attirés par des images dont la dimension fractale se situe entre 1,3 et 1,5, ce qui est grosso modo la dimension de nombreuses formes qui existent dans la nature. Sans doute peut-on trouver dans l'évolution humaine de quoi expliquer que notre cerveau soit attiré par cette sorte de fractales. Elles correspondent à des formes que nos cerveaux ont appris à reconnaître, à force d'évoluer dans un contexte donné. Ou peut-être, tout comme la meilleure musique se situe quelque part entre les extrêmes que sont l'ennuyeuse musique d'ascenseur et le bruit blanc aléatoire, ces formes nous plaisent-elles car leur complexité se situe à mi-chemin entre ce qui est trop régulier et le pur bruit aléatoire.

Si Pollock créait des fractales, sa technique est-elle pour autant facile à imiter ? En 2001, un collectionneur d'art texan pris de

doutes concernant un « Pollock » en sa possession (le tableau n'était ni signé ni daté) montra la toile aux mathématiciens qui avaient révélé la dimension fractale du style de Pollock. Selon leur analyse, la toile ne possédait pas les spécificités fractales propres au style saccadé de Pollock, et ils en conclurent qu'il s'agissait vraisemblablement d'un faux. Cinq ans plus tard, le Pollock-Krasner Authentication Board, fondé par les héritiers de l'artiste afin de vérifier l'authenticité de certaines œuvres jugées litigieuses, demanda à Richard Taylor et son équipe d'effectuer l'analyse fractale d'une collection de trente-deux peintures récemment retrouvées dans un garde-meuble, afin de confirmer qu'elles étaient bien de Pollock. L'analyse fractale conclut qu'il s'agissait également de faux.

Cela ne veut pas dire pour autant qu'il est impossible de faire un faux Pollock. Taylor est allé jusqu'à fabriquer une sorte de machine, le Pollockiser, capable de créer de véritables peintures fractales. Des pots de peinture sont reliés par des ficelles à une bobine électromagnétique programmée pour effectuer des mouvements chaotiques. Il en résulte des Pollock tout à fait convaincants. Ainsi, grâce aux mathématiques, il est possible de détecter des faux, mais aussi de créer des images susceptibles de tromper plus d'un expert.

Ayant des dimensions (comme 1,26 ou 1,72) qui ne sont pas des nombres entiers, les fractales sont indubitablement des formes étranges, mais au moins est-il possible de les dessiner. Préparez-vous maintenant à ce que les choses deviennent plus étranges encore, car notre prochaine étape est l'hyperespace et l'exploration de formes qui existent au-delà de notre monde tridimensionnel.

COMMENT VOIR DANS LA QUATRIÈME DIMENSION

Je me souviens encore à quel point j'étais excité le jour où pour la première fois j'ai « vu » en dimension 4 grâce à l'apprentissage d'un langage me permettant de visualiser mentalement ces formes. Voir en quatre dimensions est rendu possible grâce à un dictionnaire, inventé par René Descartes, qui transforme les formes en équations. Conscient que le monde visuel est souvent très

difficile à appréhender, Descartes désirait trouver un moyen mathématique simple et efficace pour faciliter cet exercice.

Ce puzzle (figure 2.35) montre que l'on ne doit pas toujours faire confiance à ses yeux. Descartes disait que la perception des sens est en réalité une tromperie des sens.

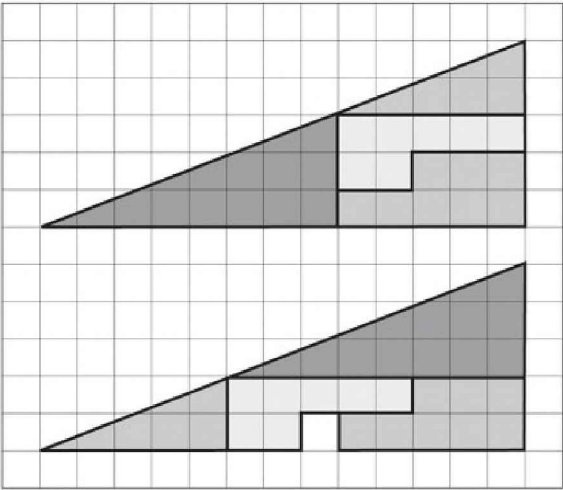


Fig. 2.35 Réorganisez les morceaux de ce puzzle et l'aire semble avoir diminué d'une unité.

Bien que la seconde image reprenne exactement les formes de la première d'une autre manière, l'aire totale semble avoir été réduite d'un carreau. Comment est-ce possible ? C'est que, alors que les hypoténuses des deux petits triangles de la figure du dessous semblent être alignées, en réalité elles sont à des angles légèrement différents, suffisamment pour que tout nouvel agencement donne l'impression qu'une unité d'aire a été perdue.

Pour faire face au problème de la perception visible, Descartes conçut un puissant dictionnaire qui traduit la géométrie en nombres et avec lequel nous sommes tous désormais familiers. Lorsque nous cherchons une ville dans un atlas, nous voyons qu'elle est associée à des coordonnées, deux nombres qui en donnent la localisation sur une grille. Ces nombres indiquent précisément l'emplacement nord/sud, est/ouest à partir d'un point sur l'équateur situé directement au sud de Greenwich à Londres.

Par exemple, Descartes est né en Touraine dans la ville de... Descartes (à sa naissance elle s'appelait La Haye), dont la latitude est 47° N et longitude 0.7° E. Dans le dictionnaire de Descartes, sa

ville natale est définie par deux coordonnées de la manière suivante : (0.7,47).

Nous pouvons utiliser un procédé similaire pour décrire les formes mathématiques. Par exemple, si nous souhaitons décrire un carré en utilisant le système des coordonnées de Descartes, je peux dire que c'est une forme ayant quatre sommets situés aux points (0,0), (1,0), (0,1) et (1,1). Chaque arête correspond au choix de deux sommets dont une seule des coordonnées varie. Par exemple, une des arêtes correspond aux deux coordonnées (0,1) et (1,1).

Le monde plat bidimensionnel n'a besoin que de deux coordonnées pour situer chaque point, mais si nous voulons également prendre en compte la hauteur par rapport au niveau de la mer, alors nous devons ajouter une troisième coordonnée. Nous aurons également besoin de cette dernière pour décrire un cube tridimensionnel en termes de coordonnées. Les huit sommets d'un cube peuvent être décrits par les coordonnées suivantes : (0,0,0), (1,0,0), (0,1,0), (0,0,1), (1,1,0), (1,0,1), (0,1,1), et finalement le point le plus loin du premier coin, situé à (1,1,1).

Encore une fois, une arête consiste en deux points dont une seule coordonnée varie. Il est facile de compter le nombre d'arêtes d'un cube que l'on a sous les yeux. Mais si on ne peut pas le voir, il suffit alors de compter combien il y a de paires de points qui diffèrent entre elles d'une seule coordonnée. Gardez cela à l'esprit lorsque nous étudierons une forme qui n'a pas d'image.

Dans le dictionnaire de Descartes, il y a, d'un côté, les formes et de la géométrie et, de l'autre, les nombres et des coordonnées. Le problème est que la partie visuelle disparaît dès lors que nous tentons d'aller au-delà des formes tridimensionnelles, puisqu'il n'y a pas de quatrième dimension physique dans laquelle nous pourrions voir des formes de dimension supérieure. La beauté du dictionnaire de Descartes, c'est que l'autre partie du dictionnaire, elle, persiste. Pour décrire un objet quadridimensionnel, il nous suffit d'ajouter une quatrième coordonnée qui indiquera jusqu'où nous nous plaçons dans cette nouvelle direction. Bien que je ne puisse jamais construire physiquement un cube quadridimensionnel, en utilisant des nombres, je peux quand même le décrire avec précision. Il a 16 sommets, commençant à (0,0,0,0), allant vers les points situés à (1,0,0,0) et à (0,1,0,0) et jusqu'au point le plus éloigné, à (1,1,1,1). Les nombres constituent un code permettant de décrire la forme, et je peux utiliser ce code afin d'explorer la forme sans que jamais il soit nécessaire de la voir physiquement.

Par exemple, combien d'arêtes a ce cube quadridimensionnel ? Une arête correspond à deux points dont seule une des coordonnées varie. À chaque sommet se rencontrent quatre arêtes, que l'on exprime en changeant chacune des quatre coordonnées, une à la fois. Cela nous donne 16×4 arêtes... mais est-ce juste ? Non, car nous avons compté chaque arête deux fois : une fois en tant qu'arête issue du sommet et une fois en tant qu'arête issue de l'autre sommet. Donc le nombre total d'arêtes dans un cube quadridimensionnel est $16 \times 4/2 = 32$. Et ce n'est pas fini. Vous pouvez aller en dimensions supérieures et construire des hypercubes. Par exemple, un hypercube de dimension N aura 2^N sommets. De chacun de ces sommets, N arêtes sont issues, et comme je compte chacune deux fois, le cube N -dimensionnel a donc $N \times 2^{N-1}$ arêtes.

Les mathématiques nous donnent un sixième sens, qui nous permet de jouer avec des formes qui existent au-delà des frontières de notre univers tridimensionnel.

OÙ PEUT-ON VOIR UN CUBE DE DIMENSION 4 À PARIS ?

Dans le cadre des célébrations du bicentenaire de la Révolution française, le président François Mitterrand commanda à l'architecte danois Johan Otto von Spreckelsen un bâtiment ambitieux situé dans le quartier de la Défense à Paris. Le bâtiment devait être construit dans l'alignement d'autres monuments célèbres de Paris — le musée du Louvre, l'Arc de triomphe et l'obélisque de la place de Concorde — afin de créer ce qui s'appellerait bientôt la « perspective Mitterrand ».

En construisant la Grande Arche, l'architecte remplit parfaitement sa mission. Ses proportions sont si immenses que les tours de Notre-Dame pourraient passer à travers, et sa masse — stupéfiante — est de 300 000 tonnes. Malheureusement, Spreckelsen est mort deux ans avant l'inauguration. Bien que ce soit aujourd'hui l'une des architectures emblématiques de la capitale, nombreux sont les Parisiens qui passent devant tous les jours sans savoir qu'ils ont devant les yeux un cube quadridimensionnel.

Cela dit, puisque nous vivons dans un univers tridimensionnel, ce n'est pas tout à fait un cube quadridimensionnel. Mais tout comme les artistes de la Renaissance relevèrent, grâce à la perspective, le défi consistant à représenter des formes tridimensionnelles sur la toile bidimensionnelle, l'architecte, à la Défense, a saisi une ombre du cube quadridimensionnel dans notre univers tridimensionnel. Afin de donner l'illusion d'un cube tridimensionnel sur une toile bidimensionnelle, un artiste pourra, par exemple, dessiner un carré à l'intérieur d'un autre carré plus grand, puis relier les coins des carrés afin de former le cube. Bien sûr, ce n'est pas vraiment un cube, mais cela donne au spectateur suffisamment d'informations : il peut voir toutes les arêtes et ainsi visualiser le cube.



Fig. 2.36 La Grande Arche de la Défense à Paris est l'ombre d'un cube quadridimensionnel.

Spreckelsen utilisa le même principe pour construire une projection d'un cube quadridimensionnel dans le Paris tridimensionnel, en plaçant un petit cube à l'intérieur d'un cube plus grand et en faisant se rejoindre les arêtes aux sommets des deux cubes. Si vous visitez la Grande Arche et comptez soigneusement les arêtes, vous pouvez voir les 32 arêtes que nous avons identifiées dans la partie précédente, grâce aux coordonnées de Descartes.

Chaque fois que je me suis rendu à la Grande Arche de la Défense, j'ai été frappé par les impressionnantes bourrasques de vent qui soufflent à travers le centre de l'arche comme pour nous y aspirer. Ce problème était tel qu'une sorte de dais en toile tendu

par des câbles fut installé afin de dévier le flot de l'air. C'est un peu comme si la construction de l'ombre d'un hypercube avait ouvert la porte vers une autre dimension.

Il existe d'autres moyens de faire l'expérience d'un cube quadridimensionnel dans notre monde tridimensionnel. Pensez à la façon dont vous construiriez un cube tridimensionnel avec un morceau de bristol bidimensionnel. D'abord, vous dessineriez six carrés formant une croix, un carré pour chacune des faces du cube. Puis, après découpe, vous plieriez la croix pour former un cube. De la même manière, il est possible dans notre monde tridimensionnel de construire un patron tridimensionnel qui, si nous avons une quatrième dimension, pourrait être plié pour former un cube quadridimensionnel.

Vous pourriez vous lancer dans la fabrication d'un cube quadridimensionnel en découpant et en assemblant huit cubes. Ce seront les « faces » de votre cube quadridimensionnel. Pour faire le patron du cube quadridimensionnel, il faut faire se rejoindre ces huit cubes. Commencez par coller ensemble les quatre premiers cubes pour former une colonne bien droite. Puis, prenez les quatre cubes restants et collez-les sur les faces d'un des quatre cubes de la colonne. Votre hypercube déplié devrait maintenant ressembler à l'intersection de deux croix, comme dans la figure 2.37.

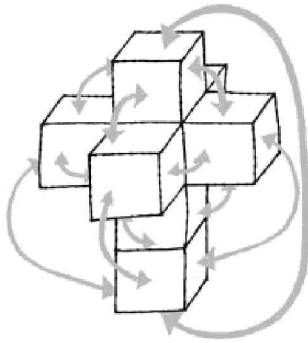


Fig. 2.37 Comment fabriquer un cube quadridimensionnel à partir de huit cubes tridimensionnels.

Pour plier le tout, il faudrait commencer par faire se rejoindre le cube du haut et le cube du bas de la colonne. Puis faire se rejoindre les carrés donnant sur l'extérieur de deux des cubes collés sur les côtés opposés de la colonne, au cube en bas de la colonne. Enfin, il faudrait coller les faces des deux autres cubes latéraux aux deux

faces qui restent sur le cube du bas. Le problème, bien sûr, c'est que dès que vous commencez à plier cette chose, vous vous emmêlez, car il n'y a tout simplement pas assez de place dans le monde tridimensionnel. Il vous faudrait une quatrième dimension pour pouvoir plier cet objet selon mes instructions.

Tout comme l'architecte à Paris a été inspiré par l'ombre du cube tridimensionnel, l'artiste Salvador Dalí était intrigué par l'idée de cet hypercube déplié. Dans sa peinture *Crucifixion (Corpus Hypercubus)*, Dalí dépeint le Christ crucifié sur le patron tridimensionnel d'un cube quadridimensionnel. Pour Dalí, l'idée d'une quatrième dimension située au-delà de notre monde matériel fait écho à celle d'un monde spirituel situé au-delà de notre univers physique. Son hypercube déplié consiste en deux croix qui se coupent, et le tableau suggère un lien entre l'ascension du Christ au ciel et la tentative de replier cette structure tridimensionnelle dans la quatrième dimension, en dépassant la réalité physique.

Quelles que soient nos tentatives pour décrire ces formes quadridimensionnelles dans notre univers tridimensionnel, jamais elles ne pourront offrir une image entière et satisfaisante, de même qu'une ombre ou une silhouette dans le monde bidimensionnel ne peuvent que donner une information partielle. Lorsque nous faisons tourner l'objet, les ombres projetées changent, mais sans que nous puissions voir le tout. Ce thème fut repris par l'écrivain Alex Garland dans son roman *Tesseract*, autre nom d'un cube quadridimensionnel. Ce récit décrit, du point de vue de chaque personnage, une même histoire centrale qui se déroule dans le milieu de la pègre à Manille. Pris individuellement, aucun point de vue ne fournit une image d'ensemble ou complète des événements, mais en rassemblant ces différents récits telles les pièces d'un puzzle, ou telles les différentes ombres projetées par une forme, on commence à comprendre l'histoire. Mais la quatrième dimension n'intervient pas seulement dans la conception de constructions architecturales, artistiques ou littéraires — il se peut qu'elle soit également la clé de la forme même de l'univers.

QUELLE EST LA FORME DE L'UNIVERS DU JEU VIDÉO ASTEROIDS ?

En 1979, la société de jeux d'arcade Atari lança le plus populaire de ses jeux vidéo, Asteroids. Le but du jeu est de détruire astéroïdes et soucoupes volantes tout en évitant d'entrer en collision avec les premières et de se faire tirer dessus par les secondes. La version arcade fut un tel succès aux États-Unis que beaucoup de centres de jeux firent modifier ces machines afin qu'elles puissent accueillir une plus grande quantité de pièces de 25 cents.

Mais c'est la géométrie du jeu qui, d'un point de vue mathématique, nous intéresse ici : en effet, dès que le vaisseau spatial s'envole et disparaît en haut de l'écran, il réapparaît comme par magie en bas de celui-ci. De la même manière, s'il vient à sortir de l'écran à gauche, il réapparaît à droite de l'écran. Que se passe-t-il ? Notre homme de l'espace est en fait coincé dans un monde bidimensionnel dans lequel tout l'univers peut être vu sur l'écran. Bien que cet univers soit fini, il n'a aucune frontière. Comme notre spationaute ne se cogne jamais contre un bord, il ne vit pas dans un rectangle, mais navigue dans un univers bien plus intéressant. Est-il possible de déterminer la forme de son univers ?

Si le spationaute sort de l'écran en haut et entre à nouveau en bas, alors ces deux bouts de son univers doivent être liés. Imaginons que l'écran de l'ordinateur soit en caoutchouc souple, afin que nous puissions le tordre et faire se rejoindre le bas et le haut. Lorsque le spationaute vole verticalement, nous pouvons voir maintenant qu'en réalité il voyage en rond comme dans un tube.

Et dans l'autre direction ? Lorsqu'il quitte l'écran à gauche, il entre à nouveau par la droite, donc les deux extrémités du tube, ou du cylindre, doivent aussi être liées. Si nous marquons les points où elles sont connectées, nous voyons bien que nous devons tordre le cylindre pour que le bas vienne rejoindre le haut. Conclusion : notre spationaute vit sur un bagel, un donut, ou ce que les mathématiciens appellent un tore.

Ce que j'ai illustré à l'aide de ce morceau de caoutchouc est en réalité une nouvelle manière de regarder les formes que proposèrent des mathématiciens il y a environ cent ans. Pour les Grecs de l'Antiquité, la géométrie (mot d'origine grecque signifiant littéralement « mesurer la Terre ») se cantonnait au calcul des distances entre des points et des angles. Mais ici, l'analyse de la forme de l'univers de notre jeu ne se réduit pas à la mesure de distances réelles dans cet univers, il s'agit de comprendre la manière dont le tout est relié. Cette nouvelle façon de regarder les formes — et dans laquelle je peux les étirer dans tous les sens

comme s'il s'agissait de caoutchouc ou de pâte à modeler — s'appelle la topologie.

Beaucoup de personnes utilisent des plans topologiques quotidiennement. Reconnaissez-vous le plan illustré ci-dessous (figure 2.38) ? C'est un plan géométrique du métro de Londres ; et bien qu'il soit géographiquement exact, il n'est pas très pratique pour organiser ses déplacements. Les Londoniens utilisent à la place une carte topologique, dont la première mouture, datant de 1933, est due à Harry Beck. Dans ce plan, Beck a étiré, comprimé, réaligné des éléments du plan géométrique afin d'obtenir un outil d'orientation bien plus pratique désormais connu dans le monde entier.

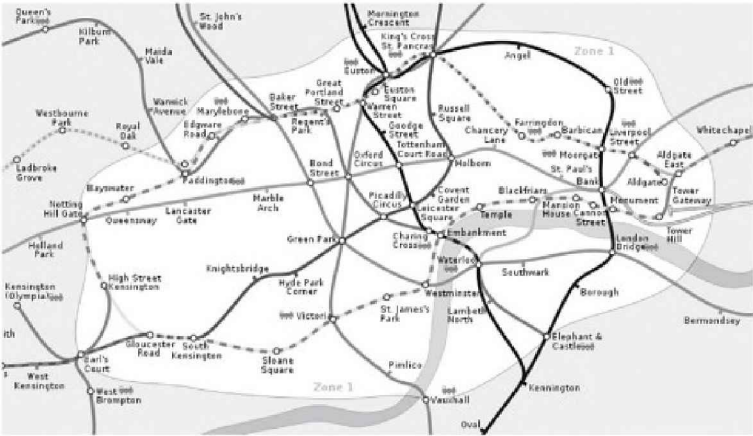


Fig. 2.38 Plan géométrique du métro de Londres.

Comprendre si un nœud peut être défait est également une question de topologie, car nous sommes autorisés à tirer les cordes dans tous les sens mais pas à les couper. C'est d'une importance capitale pour les biologistes et les chimistes car l'ADN humain a tendance à se replier pour former des nœuds étranges. Il est possible que certaines maladies, comme celle d'Alzheimer, soient liées à la manière dont l'ADN se noue, et les mathématiques peuvent offrir la solution de ces mystères.

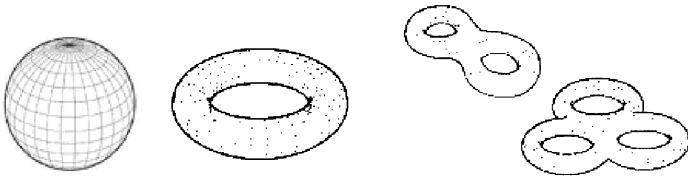


Fig. 2.39 Les quatre premières formes de la classification topologique d'Henri Poincaré montrant comment « enrrouler » des surfaces bidimensionnelles.

Au début du XX^e siècle, le mathématicien français Henri Poincaré se posa la question du nombre de surfaces topologiquement différentes. Cela revient à regarder toutes les formes possibles que notre spationaute bidimensionnel Atari pourrait habiter. Poincaré s'intéressait à ces univers d'un point de vue topologique, donc deux univers doivent être considérés comme étant les mêmes dès lors que l'un d'entre eux peut être transformé en l'autre d'une manière continue et sans coupe. Par exemple, la surface bidimensionnelle d'une sphère est topologiquement la même que la surface bidimensionnelle d'un ballon de rugby car l'une peut être moulée pour prendre la forme de l'autre. Mais cet univers sphérique est une forme topologique différente du tore dans lequel le spationaute d'Atari navigue, car on ne peut pas transformer une sphère en un donut sans couper ou coller la forme. Mais quelles sont, alors, les autres formes ?

Poincaré parvint à démontrer qu'on peut toujours déformer de manière continue n'importe quelle surface, si compliquée soit-elle, pour la transformer en l'une des surfaces suivantes : une sphère ou un tore avec un trou, deux trous, trois trous, ou n'importe quel nombre fini de trous. D'un point de vue topologique, cela constitue la liste complète d'univers possibles pour notre spationaute vidéo. C'est le nombre de trous — ce que les mathématiciens appellent le genre — qui caractérise la surface. Par exemple, une tasse de thé est topologiquement identique à un bagel car les deux ont un seul trou. Une théière a deux trous, un dans le bec et l'autre dans l'anse, et on peut la mouler pour qu'elle ressemble à un bretzel. Il est sans doute plus difficile de comprendre pourquoi la forme dans la figure 2.40, qui a également deux trous, peut être transformée en un bretzel à deux trous. Les parties en forme d'anneaux étant entrelacées, on a l'impression qu'il faut couper la forme pour la transformer en bretzel, or ce n'est pas le cas. À la fin de ce chapitre,

j'explique comment séparer ces deux anneaux sans que nous ayons besoin de les sectionner.

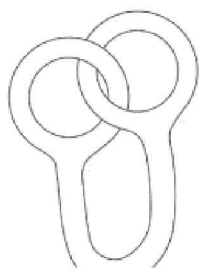


Fig. 2.40 Comment défaire ces deux anneaux entrelacés en les transformant de manière continue et sans les sectionner ?

COMMENT SAVOIR SI NOTRE PLANÈTE N'EST PAS EN FORME DE BAGEL ?

Dans les temps anciens, on pensait que la Terre était plate. Mais dès que des explorateurs commencèrent à faire de grands voyages, la question de la forme à grande échelle de la Terre devint essentielle. Si le monde était plat, alors on risquait de tomber par-dessus bord — à moins qu'il soit impossible d'atteindre le bord parce que le monde ne se finit pas.

De nombreuses cultures commencèrent à prendre conscience que la Terre était probablement courbe et finie. La plus évidente pour cette forme est bien sûr une balle, et plusieurs mathématiciens de l'Antiquité produisirent des calculs incroyablement précis concernant la taille de cette balle, fondés uniquement sur l'analyse de l'évolution des ombres au cours de la journée. Mais comment les savants pouvaient-ils être si certains que la surface de la Terre n'était pas enroulée en une autre forme intéressante ? Comment pouvaient-ils savoir que nous ne vivions pas, par exemple, sur la surface d'un immense bagel, à l'instar de notre spationaute coincé dans son univers bidimensionnel ?

Il existe pour cela un moyen qui consiste à faire un voyage imaginaire dans ces mondes alternatifs. Posons un explorateur sur la surface d'une planète et annonçons-lui qu'il s'agit soit d'une sphère parfaite, soit d'une forme parfaite de bagel. Comment peut-il faire la distinction ? Nous lui demandons de marcher tout droit

sur la surface de la planète muni d'un pinceau et d'un pot de peinture blanche, qu'il utilisera pour tracer son chemin. Au bout d'un certain temps, l'explorateur se retrouvera à son point de départ, et il aura tracé le long de son parcours un immense cercle blanc autour de la planète.

Maintenant nous lui donnons un pot de peinture noire et lui demandons de partir dans une autre direction. Sur une Terre sphérique, quelle que soit la direction qu'il prendra, le tracé noir croisera toujours le tracé blanc avant que l'explorateur n'atteigne son point de départ. Il faut se rappeler que l'explorateur avance toujours en ligne droite sur la surface. Le point où les deux chemins se croisent se situera au « pôle » à l'opposé du point d'où l'explorateur est parti.

Sur la surface d'une planète en forme de bagel, c'est une autre affaire. Le trajet avec la peinture blanche pourrait le faire aller à l'intérieur du bagel, traverser le trou et sortir de l'autre côté. Mais si, lors du trajet avec la peinture noire, il part à 90° par rapport au chemin blanc, cela l'amènerait à tourner autour du trou sans jamais y pénétrer. Donc il est possible d'entreprendre deux trajets qui ne se rencontreront qu'à l'endroit du point de départ.

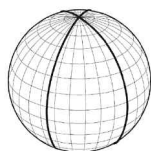


Fig. 2.41 Deux chemins sur une sphere se croisent en deux endroits.

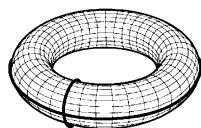


Fig. 2.42 Deux chemins sur un tore peuvent ne se croiser qu'une seule fois.

Mais la surface d'une planète n'est pas, en général, en forme de sphère ou de bagel parfaits — elle connaît quelques déformations. La surface a pu être cabossée par des météorites, modifiant ainsi sa forme générale ; par conséquent, l'explorateur qui chemine en ligne droite peut, lorsqu'il tombe sur une des ces bosses ou un de ces creux, se retrouver dévié dans une autre direction. En réalité, il est tout à fait probable que si l'explorateur marche tout droit, il ne reviendra jamais à son point de départ. Puisque ces formes bosselées ne sont néanmoins que des versions légèrement déformées de la sphère ou du bagel, peut-être existe-t-il d'autres moyens pour les distinguer. C'est là que réside toute la force de la

topologie, car elle se préoccupe moins du chemin le plus court entre deux points que de savoir si un chemin pourrait être déformé dans un autre.

Donnons désormais à notre explorateur une corde élastique blanche qu'il pose derrière lui à mesure qu'il avance, jusqu'à ce qu'il atteigne son point de départ. Une fois arrivé, il lie les extrémités de la corde comme pour faire un nœud coulant autour de la planète. Puis il repart dans une autre direction, muni cette fois d'une corde élastique noire, et marche à nouveau jusqu'à revenir à son point de départ. Si la planète est essentiellement une balle ou une sphère avec quelques creux et bosses, alors, sans avoir à couper aucune des deux cordes, il pourra toujours déplacer la corde noire afin qu'elle recouvre entièrement la corde blanche. En revanche, sur une planète en forme de bagel, cela n'est pas toujours possible. Si la corde noire passe par le trou du bagel et que la corde blanche épouse le cercle extérieur du bagel, alors il est impossible de tirer la corde noire pour qu'elle recouvre la corde blanche sans la couper. L'explorateur peut ainsi déterminer s'il y a un trou dans la planète simplement en arpentant sa surface.

Voici un autre moyen assez bizarre pour déterminer si nous nous trouvons sur une planète sphérique ou en forme de bagel. Imaginons que les deux planètes soient couvertes de fourrure. L'explorateur sur le bagel à poil constatera qu'il peut peigner la fourrure de sorte que tous les poils soient couchés dans le même sens, par exemple en coiffant les poils vers le trou et en continuant dans le même sens de l'autre côté. Mais l'explorateur sur la balle poilue ne pourra pas en faire autant. Malgré tous ses efforts, il y aura toujours un épi quelque part.

Aussi bizarre que cela puisse paraître, ce principe a des conséquences sur le temps qu'il fait sur nos deux planètes poilues. Imaginons que le sens des poils représente la direction des vents qui soufflent sur ces différents mondes. Sur le globe, il y a toujours un endroit où aucun vent ne souffle — l'épi au sommet de la tête —, mais sur le bagel le vent peut souffler sur toute la surface.

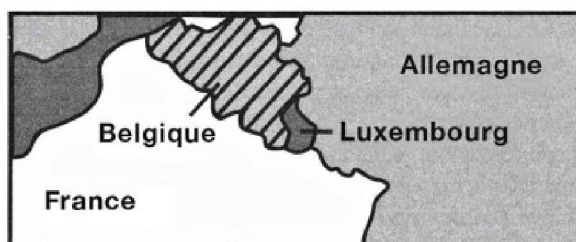


Fig. 2.43 Quatre couleurs sont nécessaires pour colorier une carte de l'Europe.

La carte que l'on peut tracer de ces deux planètes diffère aussi. Divisons chaque planète en pays puis colorions les cartes de manière à ce que deux pays ayant une frontière commune ne soient jamais de la même couleur. La carte dessinée sur la surface d'une Terre sphérique peut être coloriée à l'aide de seulement quatre couleurs. En regardant comment le Luxembourg est coincé entre l'Allemagne, la France et la Belgique, nous voyons tout de suite que nous aurons besoin d'au moins quatre couleurs. Aussi étonnant que cela puisse paraître, nous n'aurons pas besoin de plus — aucune manière de redessiner les frontières de l'Europe n'oblige les cartographes à utiliser une cinquième couleur. Mais le prouver n'a pas été une mince affaire. Pour la première fois dans le domaine des mathématiques, un ordinateur fut mis à contribution pour obtenir une preuve : colorier à la main plusieurs milliers de cartes aurait pris trop de temps.

De combien de couleurs auront besoin les cartographes de la planète en forme de bagel ? La réponse est sept maximum. Rappelez-vous le jeu vidéo et comment nous pouvons « replier » l'écran rectangulaire pour former un bagel où le haut et le bas sont reliés pour créer un cylindre horizontal, et où les côtés droit et gauche de l'écran sont reliés pour créer l'anneau du bagel. Voici une carte (figure 2.44) de la surface du bagel avant son « pliage » qui nécessite sept couleurs une fois cousue.

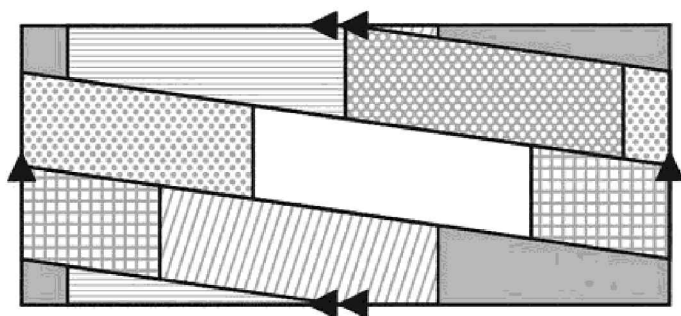


Fig. 2.44 Enroulez cette carte pour former un bagel en reliant le haut et le bas puis les deux extrémités. Vous constaterez qu'il vous faut sept couleurs.

Et maintenant, après ce voyage dans l'univers mathématique des bulles et des bagels, des fractales et des mousses, nous sommes fin prêts pour attaquer la question ultime des mathématiques des formes.

QUELLE FORME A NOTRE UNIVERS ?

Cette question n'a cessé d'obséder le genre humain depuis des millénaires. Les Grecs anciens croyaient que l'univers était enfermé dans une sphère céleste sur la paroi intérieure de laquelle étaient peintes les étoiles. Comme cette sphère faisait un tour complet toutes les vingt-quatre heures, cela expliquait le mouvement des étoiles. Cependant, ce modèle semble peu satisfaisant car, si nous devions voyager dans l'espace, rencontrerions-nous un mur à un moment donné ? Et si oui, qu'y aurait-il de l'autre côté de ce mur ?

Isaac Newton fut l'un des premiers à suggérer que l'univers n'a peut-être pas de frontières. Aussi séduisante que soit l'idée d'un univers infini, elle ne correspond pas à la théorie actuelle selon laquelle l'univers a commencé par un Big Bang et s'étend à partir d'un point concentré de matière et d'énergie. Nous pensons désormais qu'il y a une quantité finie de matière dans l'espace. Mais comment l'univers peut-il être à la fois fini et sans frontières ?

C'est là un problème semblable à celui rencontré par nos explorateurs sur un monde qui a une surface d'aire finie mais aucun bord ni frontière. Mais, au lieu d'être coincés sur une surface bidimensionnelle, nous nous trouvons au sein d'un univers

tridimensionnel. Existe-t-il une manière élégante de déterminer la forme de cet univers et de résoudre l'apparent paradoxe qui consiste à dire qu'il n'a pas de frontières tout en étant fini ?

Il fallut attendre l'invention de la géométrie quadridimensionnelle au milieu du XIX^e siècle pour qu'apparaissent des formes capables d'apporter une réponse possible. Les mathématiciens réalisèrent que la quatrième dimension leur donnait la place pour « enrouler » notre univers tridimensionnel afin de créer des formes qui soient finies en termes de volume sans pour autant avoir de frontières, tout comme la surface bidimensionnelle de la Terre ou la surface d'un bagel est finie en termes d'aire mais dénuée de bord.

Nous avons déjà vu comment un univers bidimensionnel fini tel que celui du jeu Asteroids est en réalité la surface d'un bagel tridimensionnel, mais nous, nous sommes des voyageurs tridimensionnels qui pouvons voyager dans une troisième dimension. Peut-être que l'univers dans lequel nous vivons se comporte comme celui d'Asteroids ? Pour commencer, imaginons que l'on prenne une photographie de l'univers juste après le Big Bang, quand il était encore de la taille de votre chambre à coucher. Cet univers grand comme une chambre a un volume fini, mais il n'a pas de frontières — car la chambre est « reliée » à elle-même d'une assez curieuse manière.

Imaginez que vous vous teniez au milieu de cette pièce, face à un mur (je pars du principe que votre chambre est cubique). Quand vous avancez, au lieu de vous cogner dans le mur d'en face, vous le traversez et ressortez par le mur derrière vous. De la même manière, lorsque vous traversez en marchant à reculons le mur derrière vous, vous surgissez de dos du mur en face de vous. Si vous changez de direction de 90°, et allez vers le mur à votre gauche, alors quand vous le traversez vous surgissez à travers le mur sur la droite et vice versa. La manière dont nous avons entrelacé, connecté votre chambre est donc exactement comme dans le jeu Asteroids.

Mais en tant que voyageurs de l'espace tridimensionnel, nous pouvons prendre une troisième direction. Lorsque nous volons vers le plafond, au lieu de rebondir, nous le traversons et nous retrouvons en train d'émerger du sol. Inversement, si nous traversons le sol, nous nous retrouvons en train de revenir par le plafond.

La forme de cet univers est en réalité la surface d'un bagel quadridimensionnel, ou hyperbagel, mais tout comme le

spationaute qui, coincé dans le jeu vidéo, ne peut sortir de son monde bidimensionnel pour voir comment son univers s'enroule sur lui-même, nous non plus ne pouvons voir cet hyperbagel. Cependant, grâce au langage des mathématiques, nous pouvons faire l'expérience de sa forme et en explorer la géométrie.

Maintenant, notre univers a largement dépassé la taille d'une chambre, mais il est peut-être encore replié sur lui-même comme un hyperbagel. Pensez à la lumière qui voyage en ligne droite depuis le Soleil. Peut-être qu'au lieu de disparaître dans l'infini, cette lumière fait en réalité une boucle et revient frapper la Terre. Dans ce cas, le Soleil serait une des lointaines étoiles que l'on aperçoit dans l'espace, vu de l'autre côté, puisque la lumière aurait voyagé tout autour de l'hyperbagel pour revenir enfin sur la Terre. Nous serions en train de regarder notre propre Soleil quand il était bien plus jeune.

Cela paraît incroyable, mais imaginez que vous soyez assis dans votre mini-univers (votre chambre bagel) et que vous craquiez une allumette. Si vous regardez droit devant, vous voyez la lumière de la flamme immédiatement devant vous. Maintenant, tournez-vous. Lorsque vous regardez le mur opposé de votre chambre, vous voyez encore l'allumette, seulement un peu éloignée, car la lumière de la flamme traverse le mur qui était devant vous et réémerge à travers le mur du fond de la chambre avant d'atteindre votre œil.

Au lieu de vivre sur un hyperbagel, nous pourrions tout aussi bien habiter sur la surface d'un ballon de foot quadridimensionnel. Certains astronomes pensent que nous habitons peut-être sur une forme qui ressemble à un dodécaèdre à 12 faces où, tout comme dans votre mini-univers-chambre, lorsque vous rencontrez une des faces du dodécaèdre vous re-pénétrez l'univers de la face opposée. Peut-être avons-nous bouclé la boucle pour revenir au modèle que Platon proposait il y a deux mille ans, selon lequel notre univers serait contenu dans une sorte de dodécaèdre en verre avec des étoiles collées sur sa surface. Peut-être que les mathématiques modernes peuvent élucider ce modèle, dans lequel les faces de cette forme créent, en se rejoignant, un univers sans murs de verre.

Mais l'univers pourrait-il avoir d'autres formes encore ? Souvenons-nous que Poincaré a classé toutes les formes que peut prendre une surface bidimensionnelle, telle que celle de notre planète. La surface peut être « enroulée » comme un ballon de foot, un bagel, un bretzel avec deux trous, trois trous ou plus. Poincaré a prouvé que toutes les autres formes qu'on tenterait de créer peuvent être transformées en balle ou en bretzel.

Mais qu'en est-il de notre univers tridimensionnel : quelle forme pourrait-il avoir ? C'est la « conjecture de Poincaré », le problème à un million de dollars de ce chapitre. En 2002, on annonça que le mathématicien russe Grigori Perelman l'avait résolu. Sa preuve a été vérifiée par de nombreux mathématiciens et il est maintenant reconnu qu'il a effectivement produit une classification de toutes les formes possibles de l'univers. Ce fut le premier problème à un million à être trouvé. En juin 2010, lorsque Perelman se vit présenter l'argent du prix, il le refusa, déclarant que la véritable récompense n'était pas l'argent mais le fait d'avoir résolu un des plus importants problèmes de l'histoire des mathématiques. Il avait déjà renoncé à la médaille Fields, l'équivalent pour les mathématiciens du prix Nobel. À une époque dominée par le culte de la célébrité et le matérialisme, il y a quelque chose d'assez noble dans l'attitude de cet homme pour lequel le but suprême n'est pas de gagner des prix mais de résoudre de grands problèmes.

En acceptant la preuve de Perelman, les mathématiciens connaissent désormais les formes que notre univers pourrait avoir. Maintenant, c'est aux astronomes de scruter le ciel nocturne pour déterminer laquelle correspond le mieux à son insaisissable forme.

SOLUTIONS

Imaginer des formes

La coupe sectionne les six faces, et chaque face contribue par une arête à la nouvelle face. La forme doit être symétrique, alors on obtient un hexagone.

Délier deux anneaux

Voici comment délier deux anneaux entrelacés en les transformant de manière continue en un tore à deux trous :

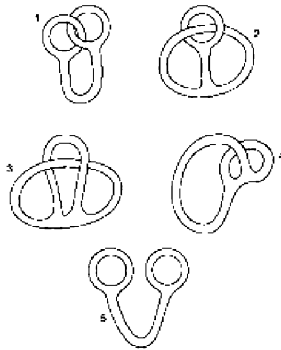


Fig. 2.45

Chapitre III

LE SECRET DES COUPS GAGNANTS

Jouer fait partie de l'expérience humaine. Les jeux constituent un moyen sans danger d'explorer les situations de la vraie vie. Le Monopoly est un microcosme de l'économie, les échecs un champ de bataille 8 sur 8, le poker un exercice d'évaluation des risques. Les jeux développent notre capacité à anticiper des événements et à nous organiser pour agir au mieux. Grâce à eux, nous apprenons à connaître le rôle que jouent la chance et l'indéterminisme qui sont au cœur du jeu de la vie.

Des civilisations anciennes du monde entier, nous avons hérité une diversité fascinante de jeux. Galets lancés dans le sable, bâtons jetés en l'air, jetons placés dans les creux d'un bloc de bois, mains utilisées pour s'affronter, images dessinées sur des cartes. De l'ancien awalé au Monopoly, du jeu de go japonais aux tables de poker de Las Vegas, quel que soit le jeu, le vainqueur est très souvent celui qui a su aborder le jeu avec une approche analytique, mathématique. Dans ce chapitre, je vous montrerai comment les maths sont le secret des coups gagnants.

COMMENT DEVENIR LE CHAMPION DU MONDE DE PIERRE-FEUILLE-CISEAUX

Jan-ken-pon au Japon. *Ro-sham-bo* en Californie. *Kai-bai-bo* en Corée. *Ching-chog-cha* en Afrique du Sud. Dans le monde entier on joue à pierre-feuille-ciseaux.

Les règles sont très simples : à trois, chaque joueur forme avec une main un des trois objets suivants : pierre (poing fermé), feuille (main ouverte parallèle à la table) et ciseaux (deux doigts tendus

formant un V). La pierre bat les ciseaux qui battent la feuille qui bat la pierre. Si deux personnes font le même signe, on a un match nul.

La logique des deux premières règles est claire : la pierre écrase les ciseaux et les ciseaux coupent la feuille. Mais pourquoi la feuille bat la pierre ? Une feuille de papier n'offre pas beaucoup de protection contre le jet d'un caillou. Mais peut-être que cette convention remonte à la Chine ancienne, à une époque où une pétition contre l'empereur était symbolisée par une pierre. L'empereur avait pour habitude d'indiquer s'il acceptait ou non la pétition en plaçant une feuille de papier sur la pierre ou en dessous de celle-ci. Si la pierre était recouverte par la feuille, la pétition était refusée et le pétitionnaire vaincu.

Nous ne savons pas très bien à quand remonte l'origine exacte de ce jeu. On le retrouve en Extrême-Orient et chez les Celtes, et dans l'Antiquité égyptienne, où l'on jouait déjà à des jeux de doigts. Cependant, toutes ces cultures ont été précédées par un groupe de lézards qui, avant même que l'*Homo sapiens* sache brandir un poing, jouaient à ce jeu de lutte pour sa survie.

La côte ouest de l'Amérique abrite le lézard *Uta stansburiana*, plus connu sous le nom de lézard à flancs maculés. Le mâle peut être de trois couleurs — orange, bleu ou jaune — et, selon sa couleur, il met en œuvre une stratégie d'accouplement différente. Les lézards orange sont les plus forts ; ils attaquent et mettent en échec les bleus. Les lézards bleus sont plus gros que les jaunes et s'adonnent volontiers à des bagarres avec eux, qu'ils remportent. Mais bien que les jaunes soient plus petits que les deux autres sortes de lézard, ils ressemblent à des femelles, ce qui a pour effet d'embrouiller les lézards orange. Ainsi, ces derniers, occupés à se bagarrer, ne remarquent pas les lézards jaunes qui passent pourtant sous leurs yeux pour aller tranquillement s'accoupler avec les femelles. Les lézards jaunes sont parfois considérés comme des fourbes en raison de leur astuce pour tromper les lézards orange. Donc, l'orange bat le bleu, le bleu bat le jaune, le jaune bat l'orange : nous avons là une version animale de pierre-feuille-ciseaux !

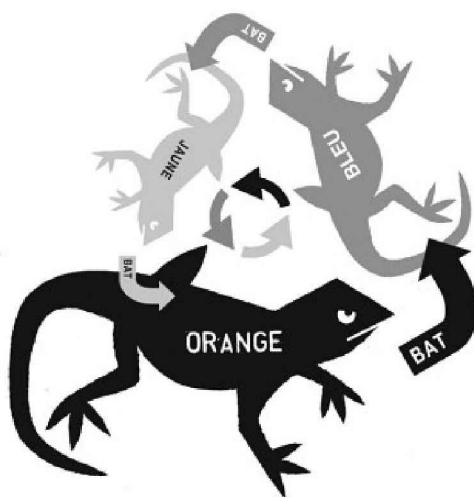


Fig. 3.01 Le lézard orange bat le bleu qui bat le jaune qui bat l'orange.

Ces lézards jouent depuis longtemps à ce jeu dans le but de perpétuer leurs gènes, et il serait intéressant de savoir s'ils ont développé une stratégie gagnante. Leur population tend à obéir à un cycle de six ans pendant lequel, dans un premier temps, les oranges dominent, puis les jaunes, puis les bleus, puis à nouveau les oranges. Le motif qui ressort est le même que celui que les gens utiliseront pour tenter de gagner à ce jeu lors d'une partie en un contre un. Voyant que votre adversaire ne cesse de vous « lancer » des pierres, vous commencez à proposer des feuilles, mais une fois que votre adversaire voit le flot de feuilles battre de manière répétée sa pierre, il se ravise et prend les ciseaux pour couper vos feuilles. Rapidement vous remarquez son changement de comportement et vous vous emparez de la pierre.

Gagner à ce jeu repose essentiellement sur notre capacité à déceler des régularités chez l'adversaire, ce qui est un trait de caractère très mathématique. Si vous êtes capable de prévoir le prochain coup de votre adversaire en vous fondant sur son profil de comportement, alors la victoire est pour vous. Le souci, c'est que vous ne voulez pas que vos réactions suivent un rythme trop évident, sinon votre adversaire prendra le dessus. La psychologie joue un rôle important dès lors que chaque adversaire s'efforce de percevoir les modèles de profils du jeu de l'autre, et tente de deviner ce qu'il s'apprête à jouer.

Depuis peu, pierre-feuille-ciseaux est passé de la cour d'école à la cour des grands lors de compétitions internationales et, chaque

année, une récompense de 10 000 dollars est offerte au champion du monde. Jusqu'à récemment, les gagnants étaient tous originaires d'Amérique du Nord, mais en 2006, le Londonien Bob « The Rock » Cooper eut l'audace de remporter le titre. Comment s'était-il entraîné ? « Plusieurs heures de répétition quotidiennes devant le miroir. » J'imagine que cela doit aider à mieux comprendre comment l'adversaire lit ce que vous avez dans la tête. Quel est le secret de son succès ? Son surnom pousse ses adversaires à croire qu'il annonce pierre plus souvent que nécessaire, ce qui lui permet de présenter ses ciseaux pour couper la feuille qui espérait le battre. Mais, une fois que ses adversaires ont compris la ruse, Bob « The Rock » opte alors pour une approche plus mathématique.

La meilleure stratégie consiste, d'un point de vue plus mathématique que psychologique, à jouer de manière aléatoire. L'adversaire n'a alors rien sur quoi fonder son prochain coup, car lors d'une séquence véritablement aléatoire, ce qui vient d'avoir lieu n'a aucune influence sur ce qui va suivre. Si je lance une pièce en l'air dix fois, les neuf premiers lancers n'influenceront pas le dixième. Même si vous avez obtenu face neuf fois, cela ne veut pas dire qu'à la dixième fois, comme pour contrebalancer la donne, vous aurez pile. Une pièce n'a pas de mémoire.

Jouer de manière aléatoire à pierre-feuille-ciseaux ne permet de gagner qu'une fois sur deux, car il n'y a aucune différence avec le jeu de pile ou face. Mais, si j'étais amené à jouer contre le champion du monde, j'adopterais volontiers n'importe quelle stratégie capable de me garantir ce niveau de chance. Je ne connais pas beaucoup de sports pour lesquels il existe une stratégie qui permet d'avoir 50 % de chances de gagner contre un champion du monde. Le 100 mètres ? Je ne crois pas.

Mais comment faire pour que les choix soient réellement aléatoires et ne cachent pas quelque motif prévisible ? C'est là un réel problème, car les humains sont très mauvais pour imaginer des séquences aléatoires ; nous sommes tellement accros à la présence d'un motif, d'une récurrence, que nous avons beaucoup de mal à empêcher des éléments structurés de s'introduire dans les suites aléatoires que nous tentons d'inventer. Pour vous aider à gagner grâce à des choix aléatoires, téléchargez sur la page Web du livre le PDF d'un dé pierre-feuille-ciseaux à assembler.

CISEAUX ET CÉZANNE

Le jeu de pierre-feuille-ciseaux est utilisé pour départager des adversaires non seulement dans la cour d'école, mais aussi dans le monde des affaires. Deux célèbres salles des ventes, Sotheby's et Christie's, sont connues pour avoir réglé, par un simple jeu de pierre-feuille-ciseaux, un important différend concernant l'organisation des enchères d'une collection de toiles signées des impressionnistes Cézanne et Van Gogh.

Les deux salles des ventes eurent le week-end pour élaborer leur stratégie. Sotheby's embaucha à grands frais une équipe de prestigieux analystes afin d'élaborer une stratégie gagnante. Ils conclurent que, le jeu étant fondé sur la chance, un choix aléatoire était ce qu'il y avait de mieux. Alors, ils décidèrent feuille. Chez Christie's, on demanda simplement à la fille de onze ans d'un des employés ce qu'elle ferait. « Tout le monde pense qu'on va dire pierre, alors ils ont dû choisir la feuille. Donc il faut choisir ciseaux », leur expliqua-t-elle. Christie's remporta le contrat.

En conclusion, les mathématiques ne vous donnent pas toujours l'avantage.

ÊTES-VOUS DOUÉ POUR L'ALÉATOIRE ?

D'une manière générale, notre intuition est mauvaise pour tirer les conséquences du hasard. Je vous propose un pari. Je vais lancer une pièce dix fois. Vous me donnez 1 euro si elle tombe sur pile ou face trois fois de suite. S'il n'y a aucune série de trois, c'est moi qui vous donne 2 euros. Vous pariez ? Non ?

Et si je vous propose 4 euros ? Si vous hésitez, je pense qu'à présent vous êtes partant. Après tout, il semble assez peu probable que la pièce tombe trois fois de suite sur pile ou sur face en lançant la pièce dix fois. Pourtant, aussi étonnant que cela puisse paraître, vous avez 82 % de chances qu'une telle suite ait lieu. J'ai donc 82 % de chances de gagner le pari, et de recevoir de vous 1 euro.

La probabilité exacte d'obtenir trois faces ou trois piles d'affilée en lançant dix fois une pièce est de $\frac{846}{1024}$. Voici maintenant les

détails pénibles du calcul. Assez bizarrement, les nombres de Fibonacci que nous avons vus au chapitre 1 constituent la clé pour déterminer ces chances — preuve supplémentaire de

l'omniprésence de ces nombres. Si je lance une pièce N fois, elle a 2^N manières d'atterrir d'un côté ou de l'autre. Admettons que g_N soit le nombre de combinaisons sans succession de trois piles ou de trois faces : c'est-à-dire les combinaisons qui vous permettent de remporter le pari. Nous pouvons calculer g_N grâce à la règle des nombres de Fibonacci :

$$g_N = g_{N-1} + g_{N-2}$$

Maintenant, sachez simplement que $g_1 = 2$ et $g_2 = 4$, car après un ou deux lancers, aucune combinaison ne peut contenir trois piles ou trois faces, car nous n'avons pas encore lancé la pièce trois fois. La séquence est donc la suivante :

2, 4, 6, 10, 16, 26, 42, 68, 110, 178

Ainsi, il existe $1\,024 - 178 = 846$ manières différentes pour une pièce lancée dix fois de tomber trois fois d'affilée sur pile ou sur face. Par conséquent, la probabilité qu'une telle suite se produise, et que je gagne, est de $\frac{846}{1024}$, soit environ 82 %.

Pourquoi la règle de Fibonacci est-elle la clé du calcul de g_N ? Prenez toutes les combinaisons de $N - 1$ lancers sans série de trois piles ou de trois faces. Il y en a g_{N-1} . Maintenant, faites que le N -ième lancer soit le contraire du $(N - 1)^{\text{e}}$ lancer. Ensuite, prenez toutes les combinaisons des lancers $N - 2$ sans série de trois piles ou de trois faces. Il y en a g_{N-2} . À présent, faites en sorte que les $(N - 1)^{\text{e}}$ et N^{e} lancers soient le contraire du $(N - 2)^{\text{e}}$ lancer. De cette manière, vous générez toutes les combinaisons de lancers sans série de trois piles ou de trois faces.

COMMENT GAGNER AU LOTO ?

C'est la question qu'on me pose le plus souvent quand je dis que je passe ma vie à jouer avec les nombres. Tout comme dans un jeu de pile ou face, les numéros tirés la semaine dernière ne peuvent en aucun cas influencer les numéros du prochain tirage. C'est là le sens même de l'aléatoire. Certaines personnes, cependant, n'arrivent pas à l'admettre.

Au loto italien, qui a lieu dans dix villes du pays deux fois par semaine, les joueurs peuvent miser sur un chiffre de 1 à 90. En 2005, cela faisait presque deux années de tirages que le numéro 53 n'était pas sorti à la loterie de Venise. Après si longtemps, se disaient les gens, il va forcément sortir au prochain coup. Leur conviction était telle qu'ils furent extrêmement nombreux à miser d'importantes sommes sur le fameux numéro. On raconte même qu'une mère de famille ayant misé, en vain, l'ensemble de ses économies sur le 53 se suicida, et qu'un homme s'endetta si lourdement après avoir à maintes reprises parié sur ce même numéro, qu'il tua femme et enfant avant de se donner la mort. Au total, les Italiens auraient misé plus de 3 milliards d'euros sur le 53.

Certaines associations demandèrent au gouvernement le retrait du 53 afin de mettre un terme à cette terrible obsession. Lorsque, le 9 février 2005, le fameux numéro sortit enfin, entre 600 et 800 millions d'euros furent partagés entre les heureux gagnants. Inévitablement, certaines personnes accusèrent le gouvernement d'avoir volontairement empêché le 53 de sortir pour éviter de payer des gains devenus importants. Ce n'était pas la première fois que survenait une telle rumeur. Déjà, en 1941, alors que, après 201 tirages le 8 n'était toujours pas sorti, de nombreuses personnes prétendirent que Mussolini l'avait tout bonnement exclu des tirages afin de canaliser les mises vers les caisses de l'État en vue de financer l'effort de guerre.

Vous avez choisi vos numéros ? Pour voir si vous avez gagné, allez sur le site Web <http://bit.ly/quickpick>

Voyons maintenant si vous avez de la chance et jouons à notre propre petite loterie. Je ne vous promets pas de gagner des millions, en revanche, la bonne nouvelle c'est que ce jeu est gratuit. Pour jouer, choisissez six numéros parmi les 49 de la grille ci-dessous.

[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
[11]	[12]	[13]	[14]	[15]	[16]	[17]	[18]	[19]	[20]
[21]	[22]	[23]	[24]	[25]	[26]	[27]	[28]	[29]	[30]
[31]	[32]	[33]	[34]	[35]	[36]	[37]	[38]	[39]	[40]
[41]	[42]	[43]	[44]	[45]	[46]	[47]	[48]	[49]	

Fig. 3.02

Pour savoir si vous avez gagné, allez sur le site Web dont l'adresse est donnée dans l'encadré ci-dessus. Sélectionnez 1 dans « *Pick 1 ticket(s)* », puis United Kingdom et National Lottery, et cliquez sur « *Pick Tickets* ». Si vous n'avez pas accès à Internet, vous trouverez en fin de chapitre un choix prédéterminé de six numéros. Ne trichez pas ! Comme pour un problème de mathématiques, c'est plus amusant de trouver soi-même la bonne réponse.

Quelles sont vos chances de choisir les six bons numéros et de gagner à la loterie ? Pour calculer les chances, vous devez déterminer combien il y a de choix possibles de six numéros distincts — appelez cela N . Ensuite, la probabilité que vous ayez choisi les numéros gagnants est 1 sur N . Pour s'échauffer, commençons par regarder combien il y a de différentes manières de choisir deux numéros. Il y a 49 choix pour le premier numéro. Pour le second, vous pouvez choisir parmi 48 numéros. Chaque choix pour le premier numéro peut être apparié avec un des 48 numéros restants ; cela nous donne donc 49×48 paires possibles de numéros. Mais attention, en réalité nous avons compté chaque choix deux fois. Par exemple, si vous choisissez 27 pour le premier numéro et ensuite 23 pour le second, c'est la même chose que si vous aviez choisi 23 en premier et ensuite 27. Donc il n'y a en fait que la moitié du nombre de paires de numéros, ce qui signifie que le nombre de paires de numéros parmi lesquelles vous pouvez choisir est $\frac{1}{2} \times 49 \times 48$.

Voyons maintenant pour six numéros. 49 choix sont possibles pour le premier numéro, 48 pour le second, 47 pour le troisième, 46 pour le quatrième, 45 pour le cinquième, et enfin 44 choix pour le sixième et dernier numéro. Donc nous avons $49 \times 48 \times 47 \times 46 \times 45 \times 44$ combinaisons de six numéros. Sauf qu'à nouveau, nous avons compté certaines combinaisons plus

d'une fois. Combien de fois par exemple avons-nous compté la combinaison 1 2 3 4 5 6 ? Eh bien, nous avons pu choisir n'importe lequel de ces six chiffres pour notre premier numéro (disons le 5). Cela nous laisse cinq numéros parmi lesquels choisir notre deuxième numéro (disons le 1), quatre numéros pour notre choix suivant (disons le 2), trois numéros pour celui d'après (disons le 6), deux choix pour l'avant-dernier numéro (disons le 4) et, enfin, le dernier numéro, qui est forcément celui qui reste (dans notre cas, le 3). Donc nous aurions pu choisir les six numéros 1 2 3 4 5 6 de $6 \times 5 \times 4 \times 3 \times 2 \times 1$ différentes manières. Cela est vrai pour n'importe quelle combinaison de six chiffres. Donc il nous faut diviser $49 \times 48 \times 47 \times 46 \times 45 \times 44$ par $6 \times 5 \times 4 \times 3 \times 2 \times 1$ pour obtenir le nombre total des différentes manières possibles de remplir la grille de loto. La réponse ? 13 983 816.

Ce nombre nous renseigne également sur nos chances de gagner, puisque c'est le nombre total des combinaisons possibles des manières dont les boules sortiront du boulier de la loterie. En d'autres termes, vos chances de choisir la bonne combinaison parmi la totalité des combinaisons possibles est de 1 sur 13 983 816.

Quelles sont les chances de n'avoir aucun bon numéro ? Cela se calcule de la même manière. Votre premier numéro doit faire partie des 43 numéros qui ne sont pas sortis, votre deuxième numéro doit être un des 42 restants, et ainsi de suite. Cela donne $43 \times 42 \times 41 \times 40 \times 39 \times 38$ combinaisons différentes. Mais chaque combinaison a été comptée $6 \times 5 \times 4 \times 3 \times 2 \times 1$ de fois. Donc, le nombre total des combinaisons qui ne comportent aucun bon numéro est $43 \times 42 \times 41 \times 40 \times 39 \times 38$ divisé par $6 \times 5 \times 4 \times 3 \times 2 \times 1$, c'est-à-dire 6 096 454. Juste un peu moins de la moitié du nombre de choix possibles n'aura aucun numéro identique à un des numéros gagnants. Pour calculer vos chances de n'avoir aucun bon numéro, divisez 6 096 454 par 13 983 816. Cela donne approximativement 0,436, c'est-à-dire 43,6 % de chances d'avoir zéro bon numéro.

Ainsi, vous avez 56,4 % de chances d'avoir au moins un bon numéro. Et pour deux bons numéros, quelles sont vos chances ? Pour le calculer, il vous faut trouver le nombre de combinaisons ayant deux bons numéros. Vous avez six choix pour le premier bon numéro et encore cinq choix pour le deuxième bon numéro. Cela fait 6×5 mais, encore une fois, il vous faut diviser par 2 afin de rectifier le fait qu'on compte les combinaisons deux fois. Pour les quatre numéros qui ne sont pas bons, vous avez un choix de 43

$\times 42 \times 41 \times 40$, qu'il vous faut diviser par $4 \times 3 \times 2 \times 1$, c'est-à-dire le nombre de manières dont vous avez compté les choses deux fois. Donc le nombre de combinaisons avec exactement deux bons numéros est

$$\left(\frac{6 \times 5}{2} \right) \times \left(\frac{43 \times 42 \times 41 \times 40}{4 \times 3 \times 2 \times 1} \right) = 1\,851\,150$$

La table 3.01 vous montre les chances de deviner juste de zéro à six numéros, probabilités toutes calculées de la même manière. Pour mieux comprendre ce que disent ces chiffres, sachez que si vous jouez une grille de loto chaque semaine, il vous faudra attendre un peu plus d'un an pour espérer obtenir au moins trois bons numéros, et environ vingt ans pour un minimum de quatre bons numéros. Si Alfred le Grand (né vers 846) avait rempli une grille de loto chaque semaine, alors ce n'est que maintenant qu'il pourrait s'attendre à voir sortir cinq bons numéros. Et enfin, si la première pensée à traverser l'esprit du premier *Homo sapiens* avait été d'aller à la maison de la presse pour acheter chaque semaine un billet de loto, alors il est possible qu'à présent il ait pu remporter le gros lot une fois.

Si vous êtes assez chanceux pour gagner le gros lot, alors pour rien au monde vous ne voudriez qu'il vous advienne ce qui arriva le 14 janvier 1995 au Royaume-Uni, alors que la loterie nationale n'avait démarré dans ce pays que neuf semaines auparavant. Le jackpot cette semaine-là s'élevait à 16 millions de livres, une somme colossale. Lorsque les six numéros sortirent du boulier, les gagnants bondirent sûrement de joie sur leur canapé. Mais au moment d'aller chercher l'argent, les 132 gagnants firent l'amère découverte qu'ils n'étaient pas les seuls à avoir une grille gagnante, et devaient partager le gros lot. Chaque gagnant obtint 122 510 livres, somme décevante au regard du jackpot.

Comment tant de personnes ont-elles pu deviner la bonne combinaison ? La raison a été évoquée précédemment lorsque j'exposais le jeu de pierre-feuille-ciseaux : nous, les humains, sommes très mauvais lorsqu'il s'agit de choisir des nombres au hasard. Étant donné que 14 millions de personnes jouent au loto chaque semaine, il y a forcément beaucoup de gens attirés par des nombres semblables, par exemple le 7, un chiffre considéré comme

porte-bonheur, ou les dates d’anniversaire de naissance ou de mariage (ce qui a pour effet d’exclure les numéros de 32 à 49). Une chose, en particulier, caractérise les choix de nombreuses personnes : le désir d’étaler de manière homogène les numéros sur la grille.

<i>Nombres de bons numéros N</i>	<i>Nombre de combinaisons avec N bons numéros</i>	<i>Probabilité d’obtenir exactement N bons numéros</i>
0	$\frac{43 \times 42 \times 41 \times 40 \times 39 \times 38}{6 \times 5 \times 4 \times 3 \times 2 \times 1} = 6\,096\,454$	$\frac{6\,096\,454}{13\,983\,816} = 0,436$ Presque 1 sur 2
1	$6 \times \frac{43 \times 42 \times 41 \times 40 \times 39}{5 \times 4 \times 3 \times 2 \times 1} = 5\,775\,588$	$\frac{5\,775\,588}{13\,983\,816} = 0,413$ À peu près 2 sur 5
2	$\frac{6 \times 5}{2} \times \frac{43 \times 42 \times 41 \times 40}{4 \times 3 \times 2 \times 1} = 1\,851\,150$	$\frac{1\,851\,150}{13\,983\,816} = 0,132$ À peu près 1 sur 8
3	$\frac{6 \times 5}{2} \times \frac{43 \times 42 \times 41 \times 40}{4 \times 3 \times 2 \times 1} = 1\,851\,150$	$\frac{246\,820}{13\,983\,816} = 0,0177$ À peu près 1 sur 57
4	$\frac{6 \times 5 \times 4 \times 3}{2 \times 3 \times 4} \times \frac{43 \times 42}{2 \times 1} = 13\,545$	$\frac{13\,545}{13\,983\,816} = 0,000969$ À peu près 1 sur 1 032
5	$\frac{6 \times 5 \times 4 \times 3 \times 2}{2 \times 3 \times 4 \times 5} \times 43 = 258$	$\frac{258}{13\,983\,816} = 0,0000184$ À peu près 1 sur 54 200
6	1	1 sur 13 983 816

Table 3.01 Les chances de deviner de 0 à 6 bons numéros à la loterie nationale.

POURQUOI LES NUMÉROS AIMENT SE REGROUPER

Voici comment calculer combien de billets de loterie ont deux numéros consécutifs. Les mathématiciens utilisent souvent une astuce qui consiste à regarder un problème à l'envers, et c'est ce que nous allons faire ici. D'abord, vous comptez les billets ne comportant pas de numéros consécutifs, puis vous retirez le résultat du nombre total de combinaisons possibles afin de trouver combien de combinaisons comportent des numéros consécutifs.

Pour commencer, choisissez au hasard six numéros de 1 à 44. (Vous n'avez le droit de choisir des numéros que jusqu'à 44, et non 49. Vous saurez pourquoi dans quelques instants.) Nommez votre choix de numéros $A(1)$, ..., $A(6)$; $A(1)$ étant le plus petit et $A(6)$ le plus grand. Maintenant, $A(1)$ et $A(2)$ pourraient être consécutifs, mais $A(1)$ et $A(2) + 1$ ne le seront pas. $A(2)$ et $A(3)$ pourraient être consécutifs mais $A(2) + 1$ et $A(3) + 2$ ne le seront pas. Donc si vous prenez les six numéros $A(1)$, $A(2) + 1$, $A(3) + 2$, $A(4) + 3$, $A(5) + 4$ et $A(6) + 5$, il n'y aura pas de nombres consécutifs. (Le fait que l'on ne puisse pas choisir un numéro supérieur à 44 devient désormais clair, car si $A(6)$ est 44, alors $A(6) + 5$ est 49.)

En utilisant cette astuce, vous pouvez générer tous les billets ne comportant pas de numéros consécutifs : il suffit de choisir six numéros de 1 à 44 et de les étaler en ajoutant un peu à chacun. Et nous voyons que le nombre de billets ne comportant pas de numéros consécutifs est le même que le nombre de combinaisons de six numéros allant de 1 à 44. Il y a :

$$\frac{44 \times 43 \times 42 \times 41 \times 40 \times 39}{6 \times 5 \times 4 \times 3 \times 2 \times 1} = 7\,059\,052$$

choix de ce type. Donc le nombre de billets ayant des numéros consécutifs est :

$$13\,983\,816 - 7\,059\,052 = 6\,924\,764$$

Voici les numéros gagnants de la semaine 9 du loto :

[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
[11]	[12]	[13]	[14]	[15]	[16]	[17]	[18]	[19]	[20]
[21]	[22]	[23]	[24]	[25]	[26]	[27]	[28]	[29]	[30]
[31]	[32]	[33]	[34]	[35]	[36]	[37]	[38]	[39]	[40]
[41]	[42]	[43]	[44]	[45]	[46]	[47]	[48]	[49]	

Fig. 3.03

Cet espacement régulier des numéros n'est pas particulièrement typique d'un agencement aléatoire : les numéros sont tout autant susceptibles d'être regroupés que l'inverse. Des 13 983 816 combinaisons possibles différentes d'un billet de loterie, 6 924 764 auront deux numéros consécutifs, soit 49,5 %, c'est-à-dire presque la moitié de toutes les combinaisons. Par exemple, lors du tirage de la semaine précédente, les numéros 21 et 22 sont sortis. Et la semaine suivante, le 30 et le 31.

Mais ne devenez pas trop accro aux numéros consécutifs. Vous pensez peut-être que 1 2 3 4 5 6 est un choix astucieux. Après tout, vous avez maintenant compris que cette combinaison a tout autant de chances que les autres d'être gagnante (ou plutôt tout aussi *peu* de chances !). Si vous remportiez le gros lot avec cette combinaison, j' imagine que vous espéreriez empocher la totalité du jackpot. Or, il semblerait que plus de 10 000 personnes au Royaume-Uni choisissent cette combinaison chaque semaine — ce qui, n'est-ce pas, prouve à quel point les Anglais sont astucieux. L'ennui, c'est que si vous gagniez au loto avec cette combinaison, il vous faudrait partager vos gains avec 10 000 autres personnes aussi astucieuses que vous...

COMMENT TRICHER AU POKER ET FAIRE UN TOUR DE MAGIE AVEC UN PROBLÈME DE NOMBRE PREMIER À UN MILLION DE DOLLARS

Les joueurs malhonnêtes et les magiciens ne battent pas les cartes comme nous autres. Mais avec une bonne dose d'entraînement, tout le monde peut apprendre à faire ce qu'on appelle le *perfect shuffle*. Ce brassage parfait des cartes consiste à couper le paquet exactement en deux tas et à intercaler

systématiquement une carte de chaque tas pour former un nouveau paquet. Si vous jouez au poker et que quelqu'un bat ainsi les cartes, vous allez passer un mauvais quart d'heure.

Imaginons quatre personnes assises autour d'une table de poker : le dealer, son complice et deux joueurs qui, ne soupçonnant rien, vont se faire « plumer ». Le dealer place quatre as sur le dessus du paquet. Après un « brassage parfait », les as sont à deux cartes les uns des autres. Après un autre brassage parfait, les as sont à quatre cartes les uns des autres — c'est-à-dire parfaitement placés pour que le dealer puisse les distribuer à son complice qui se retrouve avec un carré d'as.

Le *perfect shuffle* montre aussi tout son potentiel entre les mains d'un magicien qui sait en exploiter l'une des propriétés les plus intéressantes. Si on prend un paquet de 52 cartes et qu'on effectue un *perfect shuffle* huit fois, toutes les cartes se retrouvent à leur emplacement d'origine dans le paquet. Aux yeux du spectateur, le brassage a complètement mélangé de manière aléatoire les cartes. D'autant plus que huit mélanges dépassent largement le nombre de brassages que font la plupart des gens avant de démarrer une partie. En fait, les mathématiciens ont prouvé que pour un joueur de cartes ordinaire il suffit de seulement sept brassages pour que le paquet perde entièrement sa structure initiale et devienne aléatoire. Mais le *perfect shuffle* n'a rien d'un brassage ordinaire. Considérez le paquet de cartes comme une sorte de pièce de monnaie à huit faces, et le *perfect shuffle* comme le fait d'imposer à la pièce un huitième de tour. Après huit rotations, la pièce revient à sa position de départ.

Si un paquet contient plus de 52 cartes, combien de fois doit-on faire le *perfect shuffle* pour que les cartes retrouvent leur position de départ ? Si vous ajoutez deux jokers et faites le brassage parfait avec un paquet de 54 cartes, il faudra 52 mélanges pour revenir au point de départ. Mais si vous ajoutez 10 cartes, pour obtenir un total de 64 cartes, il ne vous faut plus que six *perfect shuffles* pour que les cartes reviennent à leur place initiale. Quelle arithmétique nous indique combien de fois il faut mélanger de la sorte un paquet de $2N$ cartes (le nombre doit être pair) pour que toutes les cartes reviennent à leur position de départ ?

Numérotez les cartes 0, 1, 2 et ainsi de suite jusqu'à $2N - 1$, et vous verrez que, grâce au *perfect shuffle*, la place de chaque carte double chaque fois. La carte 1 (qui est en fait la deuxième carte) devient la carte 2. Après un autre brassage, la carte 2 devient la

carte 4, puis la carte 8. Le calcul est plus simple si on donne à la première carte le numéro 0.

Où vont les cartes situées dans le bas du paquet ? La meilleure manière de déterminer l'emplacement de chaque carte consiste à imaginer une horloge avec $2N - 1$ heures dessus ; ainsi, un paquet de 52 cartes est comme une horloge avec des heures allant de 1 à 51. Si vous voulez savoir où est passée la carte 32, alors il suffit de doubler 32, en commençant par vous placer sur l'heure 32 et en comptant 32 heures, ce qui vous amène à 13 heures. Pour trouver combien de fois je dois effectuer le *perfect shuffle* pour que toutes les cartes reviennent à leur place initiale, je dois trouver combien de fois je dois doubler les nombres sur cette horloge afin que toutes les cartes reviennent à leur place. En réalité, il me suffit de regarder le numéro 1 et de calculer combien de fois je dois doubler 1 pour revenir à 1. Sur l'horloge affichant 51 heures, voici ce que j'obtiens en répétant le doublement de 1 :

$$1 \rightarrow 2 \rightarrow 4 \rightarrow 8 \rightarrow 16 \rightarrow 32 \rightarrow 13 \rightarrow 26 \rightarrow 1$$

Et ce qui fonctionne pour 1 fonctionnera pour tous les autres nombres car, essentiellement, effectuer huit *perfect shuffles* revient à multiplier les places des cartes par 2^8 , ce qui est la même chose que multiplier par 1, c'est-à-dire que cela laisse la carte où elle se trouve.

Combien de fois au maximum devez-vous brasser le paquet pour revenir à l'ordre initial ? Pierre de Fermat a prouvé que si $2N - 1$ est un nombre premier et que vous multipliez par 2 sur l'« horloge $2N - 1$ » (modulo $2N - 1$), alors, après $2N - 2$ doublements, vous êtes certain de revenir là où vous avez commencé. Donc, pour un paquet de 54 cartes, étant donné que $54 - 1 = 53$ est un nombre premier, 52 *perfect shuffles* suffiront.

En revanche, si $2N - 1$ n'est pas un nombre premier, nous avons besoin d'une formule un peu plus compliquée pour calculer le nombre maximum de *perfect shuffles*. Si $2N - 1 = p \times q$, où p et q sont des nombres premiers, alors $(p - 1) \times (q - 1)$ est le nombre maximum de brassages nécessaires pour que le paquet retrouve son ordre initial. Ainsi, pour un paquet de 52 cartes, $52 - 1 = 3 \times 17$, et donc $(3 - 1) \times (17 - 1) = 2 \times 16 = 32$ *perfect shuffles* devraient certainement suffire ; mais, en fait, vous pouvez vous satisfaire de huit brassages parfaits. (Dans le chapitre suivant, je prouverai le tour de passe-passe de Fermat et expliquerai comment

ce procédé mathématique est au cœur des codes utilisés pour protéger des secrets sur Internet.)

ASTUCE POUR JOUER AU POKER

Dans une variante populaire du poker appelée Texas Hold'em, chaque joueur se voit distribuer deux cartes face cachée sur la table. Le dealer pose alors cinq cartes face visible sur la table. Chaque joueur doit choisir les cinq meilleures cartes parmi les deux qu'il tient et les cinq qui sont sur la table afin d'avoir une meilleure main que ses adversaires. Si on vous distribue deux cartes consécutives (disons le 7 de trèfle et le 8 de pique), peut-être allez-vous espérer faire une quinte (cinq cartes consécutives dans n'importe quelle couleur, par exemple 6 7 8 9 10).

Une quinte est une main qui a beaucoup de valeur, justement parce que les chances d'en avoir une sont plutôt minces, donc vous pensez peut-être que le fait d'avoir reçu deux cartes consécutives vous autorise à prendre le risque de tenter une quinte. Et c'est là qu'il faut vous rappeler l'astuce concernant la loterie. Deux numéros consécutifs sortent très souvent au loto, et c'est également vrai au poker. Saviez-vous que plus de 15 % des mains en première distribution dans le jeu de Texas Hold'em contiennent deux cartes consécutives ? Mais un peu moins d'un tiers de celles-ci finiront en quinte lorsque le dealer aura placé les cinq cartes communes sur la table.

Voici une question mathématique vieille de deux cents ans et remontant aux travaux de Gauss : y a-t-il infiniment de nombres N tels qu'un paquet de $2N$ cartes a effectivement besoin du nombre complet de *perfect shuffles* ? Cette question est liée à l'hypothèse de Riemann, la question proposée pour un million de dollars concernant les nombres premiers, citée en fin de chapitre 1. Si les nombres premiers sont distribués comme l'hypothèse de Riemann le prédit, alors il y aura un nombre infini de paquets de cartes à jouer nécessitant le nombre maximum de brassages. Les magiciens et amateurs de jeux d'argent du monde entier ne retiennent sans doute pas leur souffle en attendant de connaître la réponse, mais les mathématiciens sont, eux, curieux de savoir comment les nombres premiers peuvent être liés à des histoires de brassage de cartes à jouer. Et ce lien n'aurait rien de surprenant, car les nombres premiers sont si fondamentaux qu'ils surgissent aux endroits les plus inattendus.

LES MATHÉMATIQUES AU CASINO : DOUBLER OU PERDRE ?

Vous êtes au casino devant une table de roulette et vous avez 20 jetons. Vous voulez tenter de doubler votre mise avant de partir. Pour cela, vous devez placer correctement votre jeton, sur le rouge ou sur le noir. Quelle est la meilleure stratégie à adopter — tout miser en un seul tour, disons sur le rouge, ou placer un seul jeton à la fois jusqu'à ce que vous ayez soit perdu tout votre argent, soit obtenu vos 40 jetons ?

Pour analyser ce problème, il faut comprendre que vous versez au casino de petites sommes pour pouvoir jouer, une fois faite la moyenne de vos gains et pertes. Si vous misez votre argent sur le 17 noir et qu'il sort, alors le casino vous rend votre jeton et vous en donne 35 autres. S'il y avait 36 numéros sur la roulette, ce serait un jeu équitable puisque, en moyenne, le 17 noir tomberait une fois toutes les 36 fois. Donc, si vous aviez 36 jetons et misiez sans arrêt sur le 17, au bout de 35 tours perdants en moyenne, vous gagneriez et finiriez avec les 36 jetons avec lesquels vous aviez commencé. Cependant, il y a sur la roulette européenne 37 numéros sur lesquels vous pouvez miser (de 1 à 36, plus le 0 qui n'est ni noir ni rouge), mais le casino ne paie que comme s'il y avait 36 numéros.

Puisqu'il y a 37 numéros, chaque fois que vous misez 1 euro, la banque gagne essentiellement $\frac{1}{37} \times 1\text{€}$, ce qui fait environ

0,027 centime. De temps à autre, le casino doit payer un gain très élevé à un joueur, mais il sait qu'à long terme, grâce aux lois des probabilités, il gagne de l'argent. (Les chances aux USA sont encore moindres pour les joueurs car les casinos utilisent des roulettes à 38 numéros : 1 à 36, plus 0 et 00.) Chaque mise coûte donc 0,027 centime, mais vous n'êtes pas obligé de miser uniquement sur un numéro : vous pouvez par exemple miser sur le fait que le numéro sera rouge ou noir, pair ou impair, ou situé entre le 1 et le 12. Les chances sont calculées de la même manière, et donc, quel que soit le genre de mise, celle-ci vous coûtera en moyenne 0,027 centime.

Quelle est alors la stratégie la meilleure pour doubler ses gains ? D'abord, puisque vous payez à chaque tour, la meilleure stratégie est de jouer aussi peu de fois que possible. Il existe 18 chances sur 37, un peu moins de 50 %, que le rouge tombe et que vous partiez avec deux fois votre mise ; donc, même si cela signifie que vous ne passerez pas beaucoup de temps au casino, la meilleure stratégie

pour doubler sa mise est de tout jouer en une seule fois sur le rouge.

En revanche, la probabilité de doubler votre argent en ne mettant qu'un jeton à la fois est de :

$$\frac{1 - \left(\frac{19}{18}\right)^{20}}{1 - \left(\frac{19}{18}\right)^{40}}$$

c'est-à-dire 25,3 % de chances. Vous divisez par deux vos chances d'atteindre votre but si vous jouez un jeton à la fois.

Quel est alors le meilleur endroit où placer sa mise à la roulette ? Si vous avez misé sur le rouge et que la bille tombe sur le 0, dans les casinos appliquant la règle appelée « Le Partage », le croupier vous restitue la moitié de votre mise. L'avantage de la banque est dans ce cas un peu moindre. Au bout du compte, cela vous coûte :

$$(\text{probabilité de perdre}) \times \text{la mise} - (\text{probabilité de gagner}) \times \text{gain}$$

$$= \frac{18}{37} \times 1\text{€} + \frac{1}{37} \times 0,50\text{€} - \frac{18}{37} \times 1\text{€}$$

$$= 0,0135 \text{ centime}$$

alors qu'il vous coûte 0,027 centime de jouer ailleurs sur la table de jeu. Si le casino propose cette règle, cela coûte à terme deux fois moins cher de miser sur rouge ou noir que de faire un autre type de mise.

Certains casinos proposent une autre règle, appelée « en prison ». Vous avez par exemple placé votre mise sur le rouge et la bille s'arrête sur zéro. Au lieu de prendre vos jetons, le croupier place la mise « en prison ». Si vous gagnez au coup suivant, la mise

vous est restituée (sans gain), si vous perdez, la banque récupère la mise.

Quoi qu'il en soit, il semblerait que les chances ne soient jamais réellement du côté du client. Mais peut-être existe-t-il un moyen mathématique de battre le casino ? Voici une idée appelée martingale. Commencez par placer un jeton sur le rouge. Si le rouge tombe, on vous rend votre jeton plus un autre. Si ce n'est pas le rouge qui tombe, alors misez au prochain tour deux jetons sur le rouge. Si le rouge tombe, vous récupérez vos deux jetons plus les deux que le casino vous donne. Vous avez perdu un jeton lors du premier tour, donc pour l'instant vous n'avez gagné qu'un seul jeton. Si le rouge ne tombe pas lors du deuxième tour, pariez quatre jetons au troisième tour. Si le rouge tombe, alors vous remportez quatre jetons en plus de ceux que vous avez misés. Mais vous avez déjà perdu un jeton lors du premier tour, et deux le second, cela vous laisse donc avec un gain d'un seul jeton...

Ce système implique que vous doublez votre mise à chaque fois jusqu'à ce que le rouge tombe. Le total de vos gains ne sera toujours qu'un seul jeton car si le rouge tombe au cours du N -ième tour, alors vous remportez $2N$ jetons (la quantité que vous avez mise), mais lors des précédents $N - 1$ tours, vous avez perdu $P = 1 + 2 + 4 + 8 + \dots + 2^{N-1}$ jetons. Voici une façon astucieuse de calculer la perte P . P est certainement la même chose que $2P - P$. Combien font $2P$?

$$2P = 2 \times (1 + 2 + 4 + 8 + \dots + 2^{N-1}) = 2 + 4 + 8 + 16 + \dots + 2^{N-1} + 2^N$$

Maintenant retirez $P = 1 + 2 + 4 + 8 + \dots + 2^{N-1}$. Cela donne :

$$P = 2P - P = (2 + 4 + 8 + 16 + \dots + 2^{N-1} + 2^N) - (1 + 2 + 4 + 8 + \dots + 2^{N-1}) = 2^N - 1$$

Tous les nombres de la première parenthèse, à part 2^N , sont aussi dans la seconde parenthèse, c'est pourquoi tous disparaissent lors de ce calcul (calcul que nous avons déjà rencontré lorsque nous entassions des grains de riz sur un échiquier dans notre recherche des nombres premiers au chapitre 1). Vous gagnez donc 2^N , mais vous avez perdu $2^N - 1$. Vous avez un gain net d'un jeton.

Ce n'est pas beaucoup, mais le système semble garantir qu'à un moment donné vous gagnerez — après tout, le rouge finira bien par

tomber, n'est-ce pas ? Alors pourquoi les amateurs de jeux d'argent n'utilisent-ils pas cette stratégie ? D'abord, vous auriez besoin de ressources infinies pour être certain de gagner car, théoriquement, le noir peut tomber pendant très longtemps... et même si vous aviez une énorme pile de jetons, doubler à chaque tour votre mise peut très rapidement épuiser votre stock (comme avec les grains de riz). De plus, la plupart des casinos limitent la taille des mises précisément pour éviter que des joueurs n'utilisent cette stratégie. Par exemple, si la mise maximum est de 1 000 jetons, votre stratégie va échouer après le neuvième tour puisque au dixième tour vous allez vouloir miser $2^{10} = 1\,024$ jetons, ce qui est supérieur à la limite admise.

Même lorsque la règle de la mise maximale s'applique, les joueurs commettent souvent l'erreur de croire qu'une succession de huit noirs augmente considérablement la probabilité que le rouge sorte au tour suivant. Bien sûr, la chance de voir se succéder huit noirs est incroyablement faible, une chance sur 256 en fait, mais cela n'accroîtra pas la chance de voir tomber un rouge au tour suivant : c'est toujours une chance sur deux. Tout comme la pièce qu'on lance pour jouer à pile ou face, la roulette n'a pas de mémoire.

Si vous voulez jouer à la roulette, gardez à l'esprit ce que les mathématiques des probabilités vous disent : à terme, le casino gagne toujours — même si dans le chapitre V nous verrons qu'il y a peut-être une autre manière d'utiliser les mathématiques pour vous aider à gagner des millions. Si vous n'aimez ni le poker ni la roulette, alors le craps est peut-être fait pour vous. Comme nous allons le voir maintenant, les jeux de dés ont une vieille histoire.

COMBIEN DE FACES AVAIT LE PREMIER DÉ ?

Beaucoup de jeux reposent sur le hasard. Le Monopoly, le backgammon, le jeu de l'oie et bien d'autres encore comportent un lancer de dé pour déterminer le déplacement du pion. Les tout premiers dés — des os de chevilles d'animaux — furent lancés dans l'Antiquité par les Babyloniens et les Égyptiens. Ces os atterrissaient sur l'un de leurs quatre côtés, mais les joueurs constatèrent vite qu'étant donné l'aspect irrégulier des osselets, certaines faces étaient favorisées ; ils entreprirent d'améliorer cet

objet et, ce faisant, commencèrent à explorer les différentes formes tridimensionnelles capables de donner à toutes les faces les mêmes chances.

Les premiers dés trouvant leur origine dans les os des articulations, il n'est pas vraiment surprenant que certains des premiers dés symétriques fabriqués par l'homme aient revêtu la forme d'un tétraèdre, avec quatre faces triangulaires. Un des plus anciens jeux connus à ce jour utilise ces dés en forme de pyramide : le jeu royal d'Ur.

Plusieurs exemplaires du plateau et des dés tétraédriques furent découverts dans les années 1920 par l'archéologue britannique sir Leonard Woolley lors d'une campagne de fouilles dans des tombes royales, datant de 2600 av. J.-C., de l'ancienne cité sumérienne d'Ur, dans l'actuel Irak. On pense que les plateaux étaient placés dans les tombes pour que les défunts puissent se divertir dans l'au-delà. Le plus bel exemplaire de ce jeu est visible à Londres, au British Museum. Il consiste en 20 carrés sur lesquels les participants déplaçaient leurs pions en fonction des résultats donnés par les dés tétraédriques.

Ce n'est qu'au début des années 1980 que les règles du jeu furent réellement comprises grâce à Irving Finkel qui découvrit dans les archives du British Museum une tablette cunéiforme datant de 177 av. J.-C., au dos de laquelle était gravée une image de ce passe-temps. Le jeu royal d'Ur est un ancêtre du backgammon : chaque joueur a un certain nombre de pions qu'il doit faire avancer sur le plateau. Mais, d'un point de vue mathématique, ce sont les dés associés à ce jeu qui sont les plus intéressants.

À la différence des dés cubiques qui nous sont familiers, les dés tétraédriques atterrissent avec un des sommets pointant vers le haut : il n'y a donc pas une unique face sur le dessus. C'est pourquoi deux des quatre sommets de chaque dé étaient marqués d'un point blanc. Les joueurs lançaient en l'air un certain nombre de pyramides et le score correspondait au nombre de points figurant sur les sommets pointant vers le haut. D'un point de vue mathématique, lancer ces dés revient à lancer des pièces de monnaie et à compter les « piles ».

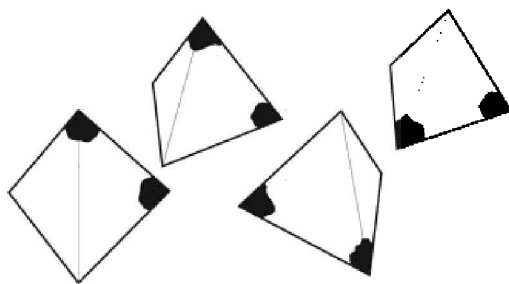


Fig. 3.04 Dés tétraédriques du jeu royal d'Ur.

Le jeu royal d'Ur dépend beaucoup du résultat aléatoire du lancer de dés ; en comparaison, le backgammon, son successeur, repose beaucoup moins sur le hasard et offre la possibilité aux joueurs d'user de leur talent stratégique. Et, bien que vieux de 5 000 ans, ce jeu n'est pas mort : il a récemment été révélé que les Juifs de Cochin, en Inde du Sud, jouent aujourd'hui encore une variante du jeu royal d'Ur.

DONJONS ET DRAGONS A-T-IL PERMIS DE DÉCOUVRIR TOUS LES DÉS ?

Donjons et Dragons, le jeu de rôles médiéval-fantastique créé dans les années 1970, avait pour originalité l'étonnante diversité de ses dés. Les inventeurs de ce jeu ont-ils découvert tous les dés possibles et imaginables ? Lorsque nous essayons de déterminer quelles formes constituent un bon dé, nous en venons à une question soulevée dans le chapitre 2. Si toutes les faces du dé ont une même forme symétrique et sont agencées de sorte que les sommets et les arêtes soient identiques, alors il existe cinq dés correspondant à cette description : le tétraèdre, le cube, l'octaèdre, le dodécaèdre et l'icosaèdre — les solides de Platon (voir p. 101 *et sq.*). Vous trouverez tous ces dés dans le coffret Donjons et Dragons, mais la plupart ont une origine bien plus lointaine.

Ainsi ce dé en verre à 20 faces (icosaèdre) datant de l'Antiquité romaine qui fut vendu chez Christie's en 2003. D'étranges symboles gravés sur ses faces suggèrent que ce dé fut utilisé pour prédire l'avenir et non pour jouer. C'est aussi un icosaèdre qui est au cœur d'un des jeux les plus populaires aux États-Unis, la « Magic 8

Ball ». Dans cette sorte de boule de cristal aux allures de boule de billard portant le numéro 8, un icosaèdre flotte dans un liquide bleuâtre. Sur chacune de ses faces est inscrite une réponse (allant de « sans aucun doute » à « une chance sur deux » en passant par « n’y compte pas »). Le principe consiste à poser une question, puis à secouer la boule : quelques instants plus tard, une des faces de l’icosaèdre vient se plaquer contre le petit hublot de la boule et la réponse s’affiche.

Si vous voulez simplement un dé qui soit juste, pas besoin d’être très strict quant à l’agencement des faces. Par exemple, on utilise dans Donjons et Dragons un dé créé en fusionnant les bases de deux pyramides à base pentagonale. Ce dé a 1 chance sur 10 d’atterrir sur n’importe laquelle de ses dix faces triangulaires. Ce n’est pas un solide de Platon car le sommet de chaque pyramide n’est pas identique aux autres sommets : cinq triangles s’y rejoignent, tandis que chaque sommet de la région où les deux bases se rencontrent est formé de quatre triangles. Mais cela reste un excellent dé.

Les mathématiciens se sont intéressés aux autres formes qui pourraient constituer des dés équilibrés. Il n’y a pas très longtemps, il a été prouvé que, pour peu que le dé conserve un minimum de symétrie, il était possible d’en ajouter 20 à la liste des cinq dés de Platon et qu’en tout, il existait cinq familles infinies de dés justes.

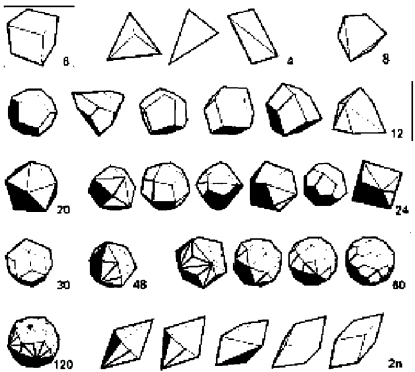


Fig. 3.05 Formes symétriques qui donnent de bons dés.

Parmi ces 20 dés en plus, 13 sont associés aux formes qui font de super ballons de foot, les solides d’Archimède vus dans le chapitre 2 (dont les faces sont symétriques mais pas nécessairement toutes les mêmes). Ces formes donnent de très

bons ballons de foot mais elles ne sont pas parfaites pour des dés. Le ballon de foot classique a 32 faces, dont 12 pentagones et 20 hexagones. Ne pourrions-nous pas faire un dé équilibré en inscrivant tout simplement les numéros 1 à 32 sur les faces ? Le problème est que chaque pentagone a une chance d'environ 1,98 % de sortir, tandis que chaque hexagone en a 3,81 % : ce n'est donc pas un dé satisfaisant. La formule précise permettant de déterminer cette proportion a été découverte il y a une dizaine d'années seulement. Un important travail de géométrie permet d'aboutir à cette réponse plutôt effrayante :

$$12 \times \frac{-3 + 30r \left[1 - \left(\frac{2}{\pi} \right) \sin^{-1} \left(\frac{1}{2r\sqrt{3}} \right) \right]}{-116 + 360r}$$

$$\text{où } r = \frac{1}{2} \left[2 + \sin^2 \left(\frac{\pi}{5} \right) \right]^{-\frac{1}{2}}$$

Les solides d'Archimède ne constituent donc pas des dés équilibrés, mais ils peuvent servir pour construire d'autres formes qui viennent étoffer l'éventail de dés dont disposent les amateurs de jeux. L'essentiel est de comprendre que, bien que les faces d'un solide d'Archimède puissent varier, les sommets, eux, sont tous identiques ; l'astuce consiste alors à mettre en œuvre une idée appelée « dualité » par laquelle les sommets deviennent des faces et inversement. Pour visualiser ce que donne cette opération, vous devez vous imaginer poser une carte de bristol sur chaque sommet et regarder comment toutes ces cartes s'agencent. Notez que chaque carte doit être perpendiculaire à la ligne qui va du centre de la forme vers le sommet que vous êtes en train de recouvrir. Par exemple, si vous remplacez de cette manière chaque sommet d'un dodécaèdre par une face, vous obtenez l'icosaèdre (figure 3.06).

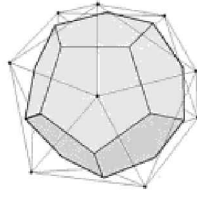


Fig. 3.06

En effectuant cela sur les solides d'Archimède, vous obtiendrez 13 nouveaux dés. Le ballon de foot classique a 60 sommets, et le dé qu'il permet de créer lorsqu'on remplace chaque sommet par une face se compose de 60 triangles, lesquels ne sont pas équilatéraux mais isocèles (deux des trois côtés sont de même longueur). Bien que ce ballon dual ne fasse pas partie des solides de Platon, il demeure néanmoins une forme où chacune des faces a 1 chance sur 60 de sortir, ce qui en fait un dé équilibré avec lequel il est possible de jouer. Son nom technique est le pentakidodécaèdre (figure 3.07).

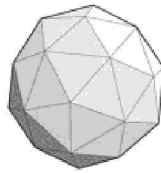


Fig. 3.07

Tous les solides d'Archimède peuvent être utilisés pour créer un nouveau dé tel que celui-ci. Le plus impressionnant est sans doute l'hexaki-icosaèdre. Même avec ses 120 triangles irréguliers à angle droit, cette forme constitue un dé équilibré.

Les familles infinies de dés se fondent sur l'idée de coller deux pyramides ensemble, quel que soit le nombre d'arêtes de leur base. Bien que l'éventail des dés symétriques et justes ait été identifié, un mystère demeure concernant les formes plus irrégulières constituant néanmoins des dés équilibrés. Par exemple, si je prends un octaèdre et que je coupe un petit bout d'un sommet puis du sommet opposé, deux nouvelles faces apparaissent. Si je jette le dé, ces nouvelles faces auront peu de chances d'être en haut, mais si je coupe des bouts plus gros, ces deux faces auront plus tendance à

être en haut que les huit faces restantes. Il doit donc y avoir une coupe intermédiaire où les deux nouvelles faces ont des probabilités égales, ce qui créerait un dé équilibré à dix faces.

Cette forme n'a pas la belle symétrie du nouveau dé que nous avons fabriqué à partir des ballons de foot d'Archimède, mais elle constituerait un dé fonctionnel. Pour preuve que les mathématiques n'ont pas réponse à tout : nous cherchons encore une manière de classer toutes les formes qui peuvent être créées de la sorte et produire des dés équilibrés.

COMMENT LES MATHÉMATIQUES PEUVENT-ELLES AIDER À GAGNER AU MONOPOLY ?

À première vue, le Monopoly ressemble à un jeu de hasard. On jette deux dés et, tandis qu'on se déplace autour du plateau à bord d'une voiture ou d'un haut de forme, on achète un terrain par-ci, un hôtel par-là. De temps à autre, on arrive second à un concours de beauté grâce à une carte « Caisse de communauté » (et on empoche 10 euros) ou, ayant dû tirer une carte « Chance », on doit déboursier 15 euros pour excès de vitesse. Chaque fois que vous passez par la case « Départ », vous gagnez 200 euros. Comment diable les mathématiques peuvent-elles nous aider à gagner ?

Au cours d'une partie, quelle est la case du plateau la plus visitée ? Est-ce la case « Départ », le « Parc gratuit » à l'angle opposé, ou peut-être celles du « Boulevard des Capucines » ou de l'« Avenue Foch » ? La réponse est en fait la « Prison ». Pourquoi ? Voyons toutes les possibilités : vous jetez les dés et vous vous retrouvez sur la case « Prison » en tant que « simple visiteur », ou bien vous êtes tombé sur la case « Allez en prison » ou, autre cas de figure, vous avez pioché une carte « Chance » ou « Caisse de communauté » exigeant que vous alliez en prison. Comme si tout cela ne suffisait pas à vous envoyer au trou, si par malheur vous faites trois fois de suite un double aux dés, vous devez effectuer une peine de trois tours.

Ainsi, la plupart des joueurs se retrouvent sur la case « Prison » environ trois fois plus que sur n'importe quelle autre case du jeu. Cela ne nous aide pas beaucoup pour l'instant, puisqu'on ne peut pas acheter cette case. Mais voilà où les mathématiques entrent en scène : où pensez-vous que les joueurs aient le plus de chances

d'atterrir en *sortant* de « Prison » ? La réponse dépend du lancer de dés le plus probable au moment de quitter cette case.

Chaque dé a une chance égale d'atterrir sur une des six faces. Avec deux dés, cela donne $6 \times 6 = 36$ différents lancers possibles, chacun avec la même probabilité. Mais lorsque vous analysez ces possibilités, vous vous rendez compte qu'un score de 2 ou de 12 est très improbable, car il n'y a qu'une seule façon d'obtenir ces scores, alors qu'il y en a six d'obtenir un score total de 7 (figure 3.08).

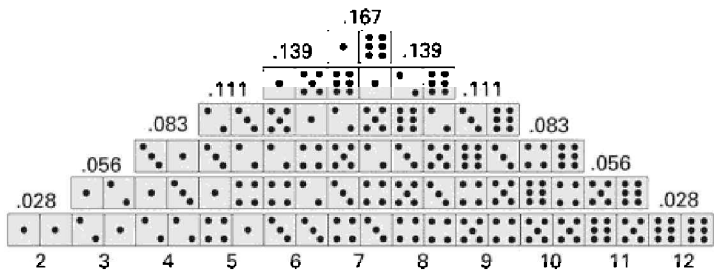


Fig. 3.08 Probabilité d'obtenir une somme avec le lancer de deux dés.

Il y a donc 6 chances sur 36, ou 1 chance sur 6, d'obtenir un 7. Ensuite, ce sont les scores 6 et 8 les plus probables. Si on obtient un 7 en quittant la « Prison », cela nous amène sur la case « Caisse de communauté », qu'on ne peut pas acheter, mais les deux propriétés orange de chaque côté (l'« Avenue Mozart » et le « Boulevard Saint-Michel ») sont les autres arrêts les plus probables.

Si vous avez la chance d'atterrir sur les propriétés orange, il faut les acheter de suite et y empiler des propriétés. Vous pourrez alors vous reposer tandis que vos adversaires vous verseront un loyer chaque fois qu'ils quittent la « Prison » et tombent chez vous.

LE GRAND JEU DES NOMBRES MYSTÉRIEUX

Ce jeu se joue à deux. Prenez 20 enveloppes et numérotez-les de 1 à 20. Le joueur 1 note 20 différents montants d'argent sur de petits morceaux de papier qu'il glisse chacun dans une enveloppe. Le joueur 2 choisit alors une enveloppe et se voit offrir le montant qu'elle contient. Il peut accepter l'argent ou choisir une autre

enveloppe. Dans ce cas, il ne peut pas revenir en arrière et réclamer le montant précédent.

Le joueur 2 continue d'ouvrir des enveloppes jusqu'à ce qu'il accepte son contenu. Le joueur 1 révèle alors tous les montants. Le joueur 2 score 20 points s'il a su choisir le montant le plus élevé. Il score 19 points s'il s'est arrêté sur le deuxième plus grand montant, et ainsi de suite.

Toutes les enveloppes sont vides, c'est maintenant au tour du joueur 2 d'écrire des montants sur des bouts de papier et de les glisser dans les enveloppes. Le joueur 1 doit lui aussi tenter de trouver le montant le plus élevé. Une fois que ce joueur s'est décidé sur une enveloppe, il établit son score selon le même principe que précédemment. Le gagnant est celui qui a le plus de points, ce qui ne signifie pas forcément le plus grand montant.

Ce qu'il y a d'intrigant dans ce jeu, c'est que vous ne connaissez pas l'éventail des montants à gagner : le premier prix pourrait tout aussi bien être 1 euro que un million d'euros. La question est la suivante : existe-t-il une stratégie mathématique capable d'augmenter vos chances de remporter la partie ? Et la réponse est oui. La stratégie repose sur une formule secrète qui dépend de e (pas la sorte psychédélique, mais mathématique). Le nombre $e = 2,71828\dots$ est sans doute l'un des plus célèbres nombres de tout l'univers des mathématiques, juste après l'énigmatique π , et il apparaît dès que la notion de croissance entre en jeu. Par exemple, il est intimement lié à la manière dont les intérêts s'accumulent sur votre compte en banque.

Imaginez que vous souhaitiez investir 1 euro et décidiez de comparer les taux d'intérêt proposés par différentes banques. L'une d'entre elles vous propose un taux d'intérêt de 100 % après un an, ce qui amènerait votre investissement à 2 euros. Pas mal, mais une autre banque vous propose un taux biannuel de 50 %. Après six mois, vous auriez alors 1,50 euro et, après un an, $1,50 \text{ €} + 0,75 \text{ €} = 2,25 \text{ €}$, ce qui est mieux. Une troisième banque propose un taux de 33,3 % cumulatif chaque tiers d'année, ce qui donne $(1,333)^3 \text{ €} = 2,37 \text{ €}$ après 12 mois. Plus vous divisez l'année en périodes courtes, plus les intérêts composés sont à votre avantage.

À ce stade, le mathématicien qui sommeille en vous se sera, espérons-le, rendu compte que la banque qu'il vous faut vraiment est la Banque de l'Infini, laquelle divise l'année en unités de temps infiniment petites, ce qui garantit le solde maximum possible. Plus vous divisez l'année, plus le solde augmente. Il ne devient pas infini

mais tend vers ce nombre magique, $e = 2,71828...$ Comme π , e a un développement décimal infini (indiqué par les « ... ») qui n'est pas périodique. Il constitue la clé pour vous aider à gagner au jeu des « nombres mystérieux ».

L'analyse mathématique de ce jeu implique que vous calculiez en premier lieu $\frac{1}{e}$, qui vaut environ 0,37. Il vous faut commencer par ouvrir 37 % des enveloppes, soit à peu près sept d'entre elles. Continuez d'ouvrir les enveloppes, mais arrêtez-vous dès que vous tombez sur un montant qui dépasse tous ceux découverts dans les autres enveloppes que vous venez d'ouvrir. Selon notre principe mathématique, une fois sur trois vous êtes sûr de décacheter l'enveloppe avec le montant le plus élevé. Cette stratégie ne sert pas seulement pour ce jeu, de nombreuses décisions dans notre vie de tous les jours peuvent être prises utilement en suivant cette stratégie.

Vous souvenez-vous de votre premier petit ami ou première petite amie ? Vous pensiez sans doute qu'il (ou elle) était super. Peut-être rêviez-vous de passer le reste de votre vie avec lui (ou elle), pour ensuite vous sentir taraudé par l'idée que vous pourriez trouver mieux ? Le problème, c'est que si vous plaquez votre partenaire du moment, c'est, en règle générale, définitif ; donc à quel moment devez-vous déclarer forfait et vous contenter de qui vous avez ? La recherche d'un appartement est un autre exemple classique. Combien de fois avez-vous vu un appartement génial dès votre première visite, mais vous avez estimé qu'avant de vous engager, il serait préférable d'en voir d'autres, au risque de perdre le premier ?

De façon surprenante, le même calcul mathématique qui vous aide à gagner au jeu des nombres mystérieux peut vous permettre de trouver le meilleur partenaire ou le meilleur appartement. Disons que vous ayez commencé à sortir avec quelqu'un vers l'âge de seize ans et que vous décidiez que d'ici l'âge de cinquante ans vous devez avoir trouvé le grand amour. Partons ensuite du principe que vous changez de partenaire à un rythme constant et régulier. Les mathématiciens vous diront que pendant 37 % du temps que vous vous êtes alloué vous devez faire un état des lieux de l'offre, ce qui vous amène aux alentours de vingt-huit ans. Puis, vous devez choisir le prochain partenaire qui vous semble meilleur que tous ceux avec lesquels vous êtes sorti jusqu'alors. Pour une personne sur trois, c'est la garantie d'aboutir au meilleur partenaire

possible. Mais attention à ne pas révéler votre méthode à l'amour de votre vie !

COMMENT GAGNER À LA ROULETTE CHOCOLAT-PIMENT

Même si les mathématiques n'ont plus de secrets pour vous, des jeux comme le Monopoly ou celui que nous venons de faire reposent en partie sur le hasard. Voici, en revanche, un jeu très simple pour deux joueurs, qui illustre comment les mathématiques peuvent vous faire gagner à tous les coups. Prenez 13 barres de chocolat et un piment de chili très fort avec lesquels vous formez un tas sur la table. Chaque joueur, à tour de rôle, prend un, deux ou trois items du tas. Le but du jeu est de contraindre votre adversaire à prendre le piment.

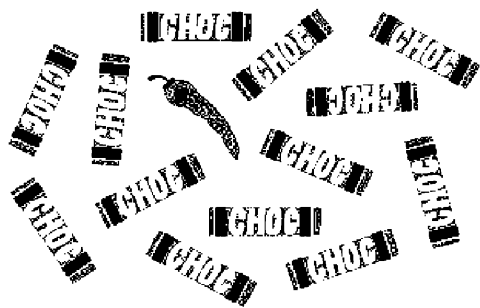


Fig. 3.09 La roulette chocolat-piment.

À condition d'être le premier à jouer, il existe une stratégie infaillible pour que votre adversaire se retrouve avec le piment. Quel que soit le nombre de barres de chocolat que prendra votre adversaire, vous devez retirer de la pile le nombre de barres qui, ajouté au nombre que vient juste de prendre votre adversaire, fera quatre barres. Ainsi, si votre adversaire prend trois barres, vous en prenez une, s'il en prend deux vous en prenez deux.

L'astuce consiste à se représenter mentalement les barres sous la forme de trois rangées de quatre. Or, comme au départ il y a 13 barres, cela fait trois rangées de quatre barres (égale 12), plus une barre (et le piment bien sûr). Votre premier coup donc, dès

l'ouverture, consiste à prendre cette treizième barre. Puis vous poursuivez comme décrit précédemment. Au bout de trois tours de jeu, votre adversaire est obligé de prendre le piment.

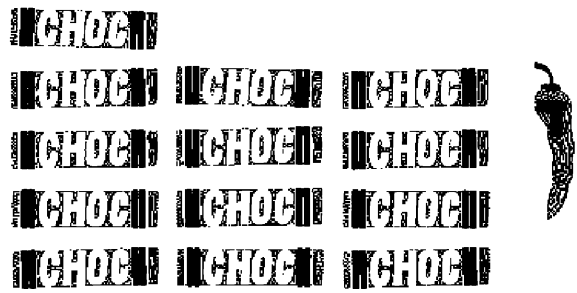


Fig. 3.10 Comment agencer les barres (mentalement) pour gagner.

Évidemment, il faut jouer le premier pour que cette stratégie fonctionne. Mais si c'est votre adversaire qui ouvre le jeu, il n'est pas très compliqué de retomber sur ses pieds. Par exemple, s'il prend plus d'une barre de chocolat dès le premier tour, il a déjà commencé à grignoter la première colonne de quatre barres ; dans ce cas, vous appliquez le principe que nous avons énoncé, et vous prenez le reste des barres de cette colonne.

Vous pouvez imaginer des variantes à ce jeu en commençant par exemple avec un autre nombre de barres de chocolat ou en modifiant le nombre maximum de barres que l'on peut prendre en une fois. La méthode mathématique consistant à diviser les barres en groupes vous permettra de concocter une stratégie gagnante.

Il existe une autre variante, baptisée Nim, dont la victoire repose sur une analyse mathématique légèrement plus complexe. Cette fois, au lieu d'un seul tas, nous en avons quatre. Un tas de cinq barres, puis un tas de quatre barres, un tas de trois barres et un dernier tas avec juste le piment. Dans cette version du jeu, vous pouvez prendre autant de barres que vous le souhaitez, mais dans un seul tas. Par exemple, vous pouvez prendre les cinq barres du premier tas, ou bien une barre du troisième tas. Encore une fois, vous perdez si vous n'avez d'autre choix que de prendre le piment.

Pour gagner à ce jeu, il faut savoir écrire les nombres en forme binaire. Nous avons appris à écrire les nombres en utilisant le système décimal, car nous comptons de 10 en 10, ayant dix doigts ; une fois arrivé à 9, nous commençons une nouvelle colonne et écrivons 10 pour indiquer une dizaine et zéro unité. Les

ordinateurs, eux, aiment compter de 2 en 2, et utilisent le système binaire. Chaque chiffre représente une puissance de 2 plutôt qu’une puissance de 10. Par exemple, 101 représente un lot de $2^2 = 4$, aucun 2 et une unité. Donc 101 est le nombre $4 + 1 = 5$ en binaire. La table ci-dessous montre quelques nombres écrits en binaire.

<i>Décimal</i>	<i>Binaire</i>
0	0
1	1
2	10
3	11
4	100
5	101
6	110
7	111
8	1000

Table 3.02 Nombres écrits en binaire.

Pour gagner au jeu de Nim, il vous faut traduire le nombre de barres de chocolat de chaque tas en binaire. Le premier tas a 101 barres, le deuxième 100 barres, le troisième 11 barres. En écrivant ce dernier chiffre 011, et en posant les trois nombres les uns en dessous des autres, on obtient :

1	0	1
1	0	0
0	1	1

Notez que la première colonne a un nombre pair de 1, la deuxième un nombre impair de 1 et la troisième un nombre pair de 1. Pour gagner, il faut, à chacun de vos tours, prendre le nombre de barres d’un tas de telle manière que chaque colonne finisse toujours avec un nombre pair de 1. Donc, dans notre cas, retirez

deux barres du troisième tas, qui en comptait trois, pour réduire le nombre de barres à 001.

Pourquoi cela vous aidera-t-il à gagner ? Eh bien, à chaque tour, votre adversaire sera obligé de laisser au moins une des colonnes avec un nombre impair de 1. Votre prochain coup consiste alors à prendre le nombre de barres nécessaire afin que toutes les colonnes aient à nouveau un nombre pair de 1. Le nombre de barres ne cessant de baisser, à un moment donné, vous ou votre adversaire allez retirer des barres et obtenir des tas qui afficheront 000, 000, 000. Duquel de vous deux s'agira-t-il ? Comme votre adversaire laisse toujours un nombre impair de 1 dans au moins un des tas, alors c'est forcément vous qui avez joué ce coup. Votre adversaire se retrouve avec le piment.

Cette stratégie fonctionne quel que soit le nombre de barres de chocolat de chaque tas, et il est même possible d'augmenter le nombre de tas.

**POURQUOI LES CARRÉS MAGIQUES PEUVENT
FACILITER
UN ACCOUCHEMENT,
EMPÊCHER LES INONDATIONS
ET GARANTIR UNE VICTOIRE AU JEU**

La pensée latérale peut s'avérer pratique en matière de mathématiques. En regardant un problème avec un point de vue légèrement différent, la réponse peut soudain apparaître totalement évidente. Pour cela, il faut savoir identifier la bonne manière d'envisager le problème. Pour illustrer ce point, voici un jeu qui est plutôt compliqué à première vue mais qui devient plus simple lorsque nous l'abordons sous un autre angle. Pour jouer à ce jeu, vous pouvez télécharger sur la page Web dédiée au livre les éléments dont vous aurez besoin et les découper.

Chaque participant a un plat à gâteau vide d'une capacité de 15 parts. Le but du jeu est d'être le premier à remplir le plat avec exactement trois morceaux de gâteau choisis parmi neuf morceaux de tailles différentes, le plus petit correspondant à une part, et le plus gros étant l'équivalent de neuf parts. Les participants choisissent à tour de rôle un des morceaux.

L'objectif est de viser trois nombres allant de 1 à 9 qui, en s'additionnant, font 15, tout en suivant ce que votre adversaire

manigance pour tenter de le mettre en échec. Ainsi, si votre adversaire a d'abord choisi un morceau de trois parts puis un autre de huit parts, alors vous devez l'empêcher de faire 15 en prenant le morceau à quatre parts. Si le morceau que vous vouliez est pris, vous devez trouver un autre moyen d'atteindre 15 en tenant compte des morceaux que vous avez déjà et de ceux qui restent à prendre. Mais vous devez utiliser précisément trois morceaux pour remplir votre plat !

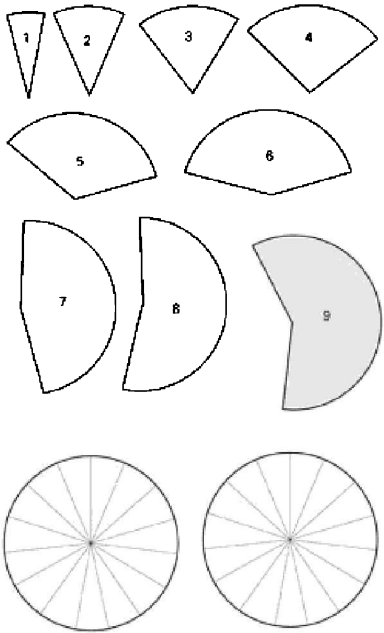


Fig. 3.11 Choisissez trois morceaux de gateau pour remplir votre plat avant que votre adversaire ne remplisse le sien.

Une fois la partie démarrée, il devient vite difficile de suivre toutes les différentes manières que vous ou votre adversaire pourriez mettre en œuvre pour remplir le plat. Mais le jeu devient plus facile dès lors que vous réalisez que vous êtes tout simplement en train de jouer au morpion ; certes, un morpion déguisé. Au lieu de la grille habituelle 3×3 dans laquelle vous placez vos ronds et vos croix dans le but d'en aligner trois avant votre adversaire, ce jeu se déroule en fait sur un carré magique :

2	9	4
7	5	3
6	1	8

Table 3.03

Le carré magique le plus basique consiste à agencer des nombres de 1 à 9 sur une grille de 3×3 afin que la somme des nombres d'une colonne, d'une rangée ou d'une diagonale soit toujours égale à 15. En envisageant le jeu du gâteau comme un morpion joué sur ce carré magique, la personne qui a trois nombres alignés a, la première, les trois nombres dont l'addition fait 15.

Selon la légende, le premier carré magique fut inscrit vers 2000 av. J.-C. sur le dos d'une tortue venue de la rivière Luo en Chine. La rivière était sortie de son lit et l'empereur Yu ordonna des sacrifices afin d'apaiser le dieu rivière. Le dieu répondit en envoyant une tortue sur la carapace de laquelle était gravé un tableau de nombres destiné à aider l'empereur à maîtriser la rivière. Dès lors que ce carré d'ordre 3 fut découvert, les mathématiciens chinois s'efforcèrent d'en construire de plus grands fonctionnant sur le même principe. Des propriétés magiques étaient attribuées à ces carrés et leur utilisation dans l'art de la divination se répandit. Les mathématiciens chinois réussirent l'exploit de concevoir un carré magique de 9×9 .

Il semblerait que ces carrés fussent exportés en Inde par des marchands chinois qui se consacraient non seulement au commerce des épices mais aussi à celui des idées mathématiques.

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Fig. 3.12 Le carre magique d'Albrecht Durer.

La manière dont les nombres sont imbriqués dans les carrés faisait écho à la croyance hindoue en la réincarnation, et, en Inde, ces carrés avaient de nombreuses fonctions ; ils étaient par exemple utilisés pour faciliter un accouchement ou pour concevoir des parfums. Les carrés magiques étaient également populaires dans la culture islamique médiévale. Grâce à leur manière systématique d'aborder les mathématiques, les Arabes avaient trouvé un moyen astucieux de générer des carrés magiques, ingéniosité qui atteignit son paroxysme au XIII^e siècle avec la découverte d'un impressionnant carré magique de 15×15 .

En Europe, l'une des premières manifestations du carré magique se trouve dans la gravure d'Albrecht Dürer intitulée *Melencolia*. Les nombres de 1 à 16 sont agencés de sorte que la somme totale d'une colonne, d'une rangée ou d'une diagonale soit égale à 34. En plus de cela, chacun des quadrants — les quatre carrés de 2×2 qui constituent le grand carré —, mais aussi le carré de 2×2 au centre, donne également une somme de 34. Dürer alla jusqu'à placer les deux nombres au milieu de la rangée du bas de manière à former l'année de création de la célèbre gravure : 1514.

Des carrés magiques de tailles diverses étaient traditionnellement associés aux planètes du système solaire. Le carré classique de 3×3 était associé à Saturne, le carré d'ordre 4 de *Melencolia* à Jupiter, et le plus grand, un carré de 9×9 , à la Lune. Selon certains historiens, Dürer aurait placé ce carré dans sa gravure afin d'exprimer une croyance mystique selon laquelle la gaieté de Jupiter pouvait tempérer le sentiment de mélancolie qui imprègne l'œuvre.

Un autre célèbre carré magique est visible à l'entrée de la flamboyante Sagrada Familia à Barcelone, cathédrale construite par Antoni Gaudí, inachevée à ce jour. Le nombre magique pour ce carré d'ordre 4 est 33, l'âge du Christ à sa crucifixion. Ce carré n'est pas aussi satisfaisant que celui de Dürer car les nombres 14 et 10 figurent deux fois, au détriment du 4 et du 16.

Les carrés magiques posent un problème que les mathématiciens ne sont toujours pas parvenus à résoudre. Il n'existe, essentiellement, qu'un carré magique de 3×3 . (Le terme *essentiellement* signifie que ce que vous obtenez par rotation ou reflet d'un carré magique n'est pas compté comme un nouveau carré.) En 1693, le Français Bernard Frénicle de Bessy fit la liste exhaustive des 880 carrés magiques d'ordre 4 possibles et, en 1973, Richard Schroepel utilisa un programme informatique pour montrer qu'il existe 275 305 224 carrés magiques d'ordre 5. Au-delà, nous n'avons que des estimations du nombre possible de carrés magiques d'ordre 6 ou plus. Les mathématiciens continuent de chercher une formule permettant de déterminer avec exactitude leur nombre.

QUI A INVENTÉ LE SUDOKU ?

L'esprit du sudoku est perceptible dans un puzzle qui est né de la fascination des mathématiciens pour les carrés magiques. Dans un jeu de cartes à jouer, prenez les figures (rois, reines et valets) et les as, et tentez de les agencer dans une grille de 4×4 afin qu'aucune rangée ni colonne n'ait une carte de même enseigne ou de même rang. Ce problème fut posé pour la première fois en 1694 par le mathématicien français Jacques Ozanam, l'homme qu'on peut considérer comme l'inventeur du sudoku.

Le mathématicien Leonhard Euler devint accro à ce problème. En 1779, quelques années avant sa mort, Euler en formula une autre version. Prenez six régiments, chacun composé de six hommes aux grades différents : disons un colonel, un capitaine, un lieutenant, un major, un caporal et un soldat. Chaque régiment porte un uniforme d'une couleur différente (rouge, bleu, jaune, vert, orange et violet). Le problème consiste à agencer les hommes sur une grille de 6×6 afin que les colonnes et les rangées ne contiennent qu'un seul grade et un seul régiment. Euler formula la

question pour une grille de 6×6 car, selon lui, on ne pouvait agencer les 36 hommes de manière satisfaisante. Ce n'est qu'en 1901 que le mathématicien amateur français Gaston Tarry apporta la preuve qu'Euler avait raison : c'est effectivement impossible.

Euler estimait également que ce puzzle était impossible à résoudre, que ce soit avec une grille de 10×10 , de 14×14 ou de 18×18 , et ainsi de suite, en ajoutant 4 chaque fois. Mais il se trompait. En 1960, avec l'aide d'un ordinateur, trois mathématiciens démontrèrent qu'il était en réalité possible d'agencer 10 différents grades de militaires appartenant à 10 régiments dans une grille de 10×10 . Au final, toutes les autres s'avèrent possibles, sauf celle de 6×6 .

Si vous souhaitez tenter la version 5×5 du puzzle d'Euler, vous pouvez télécharger le fichier *ad hoc* sur la page Web dédiée au livre. Découpez les cinq grades des cinq régiments et voyez si vous parvenez à les agencer dans la grille de 5×5 afin que chaque colonne et rangée contienne uniquement des hommes appartenant à des régiments et des grades différents. Ces carrés magiques sont parfois appelés carrés gréco-latins. Prenez les premières n lettres de l'alphabet latin et grec et notez toutes les $n \times n$ paires différentes de lettres latines et grecques. Maintenant, agencez ces paires sur une grille de $n \times n$ afin qu'aucune rangée ou colonne ne contienne la même lettre latine ou grecque.

LE CARRÉ MODE D'EMPLOI

Un des carrés gréco-latins d'ordre 10 fut utilisé par Georges Perec pour donner sa structure à son roman écrit en 1978, *La Vie mode d'emploi*. Ce livre se compose de 99 chapitres, chacun correspondant à une pièce d'un immeuble d'habitation parisien comptant 10 étages de 10 pièces chacun (une pièce, la 66°, n'est jamais visitée). Chaque pièce correspond à un emplacement sur le carré gréco-latin. Mais Perec, au lieu de prendre 10 lettres grecques et 10 lettres latines, utilise, dans un cas, 20 auteurs qu'il divise en deux listes de 10.

Lorsqu'il rédigeait le chapitre consacré à une des pièces, il regardait quels étaient les deux auteurs associés à cette pièce, et s'assurait qu'il les citait au cours dudit chapitre. Ainsi, pour le chapitre 50, le carré de Perec disait qu'il fallait citer Gustave Flaubert et Italo Calvino. Mais Perec n'utilisa pas qu'un unique carré pour écrire ce livre ; en effet, il eut recours à un total de 21 carrés gréco-latins pour décider de choses aussi diverses que le mobilier, l'époque, le style ou même la position des corps des occupants de chacune des pièces.

Un sudoku fonctionne d'une manière légèrement différente du puzzle « militaire » proposé par Euler. Dans un sudoku classique, il s'agit d'agencer neuf lots de nombres allant de 1 à 9 sur une grille de 9×9 afin qu'aucune rangée, colonne ou quadrant de 3×3 ne contienne deux fois le même nombre. La grille est préalablement remplie de quelques nombres et c'est au joueur de la compléter. Si quelqu'un vous dit que les mathématiques n'entrent pas en compte pour remplir une telle grille, ne le croyez pas. Ce qu'il veut dire, c'est que ce jeu ne repose pas sur de l'arithmétique — un sudoku est essentiellement un puzzle logique. Le genre de raisonnement logique qui vous amène à décider qu'un 3 doit être placé dans le coin en bas à droite est précisément un raisonnement mathématique.

Le sudoku pose plusieurs questions mathématiques intéressantes. Par exemple, combien existe-t-il de manières différentes d'agencer les nombres dans la grille de 9×9 pour satisfaire aux règles du jeu ? (À nouveau, il faut lire « essentiellement » différentes : on estime que le simple fait de permuter des rangées, par exemple, c'est-à-dire de modifier la grille tout en conservant sa symétrie, ne constitue pas une nouvelle grille.) En 2006, Ed Russell et Frazer Jarvis annoncèrent qu'il y avait 5 472 730 538 manières essentiellement différentes d'agencer la grille, suffisamment pour que les journaux puissent continuer à proposer des grilles sans le moindre risque de se répéter.

Un autre problème mathématique soulevé par ces puzzles n'a, quant à lui, pas été entièrement résolu. Quel est le nombre minimum de carrés pré-remplis capable d'imposer une seule et unique manière de compléter la grille ? De toute évidence, si trop peu de carrés sont pré-remplis — disons trois —, les façons de compléter la grille seront très nombreuses car il n'y aura alors pas assez d'information pour qu'existe une seule et unique solution. On estime en général qu'au moins 17 carrés doivent être prédéterminés afin de garantir l'existence d'une seule manière correcte de remplir la grille.

Ces différentes questions constituent bien plus que de simples casse-tête permettant de passer le temps. Les mathématiques sous-jacentes au sudoku ont d'importantes implications dans le domaine des codes correcteurs d'erreur, sujet que nous aborderons dans le chapitre suivant.

COMMENT LES MATHÉMATIQUES
PEUVENT-ELLES VOUS FAIRE ENTRER
DANS LE LIVRE GUINNESS
DES RECORDS ?

Il existe toutes sortes de manières délirantes d'entrer dans le Livre Guinness des records. Un comptable italien du nom de Michele Santelia parvint à y figurer en tapant à la machine 64 livres (soit 3 361 851 mots ou 19 549 382 caractères) dans leur langue d'origine et à l'envers, dont *L'Odyssée*, *Macbeth*, la Bible et le *Guinness World Records Book* de 2002. L'Anglais Ken Edwards détient le record du monde du plus grand nombre de cafards mangés en une minute – 36 –, et il fallut à l'Américain Ashrita Furman 12 heures et 27 minutes pour faire son entrée sautillante dans le livre des records après avoir parcouru pas moins de 37,18 kilomètres sur un bâton sauteur. Cet homme détient aussi le record du plus grand nombre de records ! Mais les mathématiques peuvent-elles nous aider à entrer dans le Guinness des records ?

Un des défis récurrents du Guinness depuis 1961 consiste à se rendre dans toutes les stations du métro londonien en un minimum de temps. Ce défi s'appelle le Tube Challenge et il fut relevé par Martin Hazel, Steve Wilson et Andi James le 14 décembre 2009 en un temps record de 16 heures, 44 minutes et 16 secondes. Bien qu'il s'agisse certes d'un projet a priori éreintant, une analyse mathématique du plan du métro offrira un avantage certain à quiconque souhaite battre le record, et ce en donnant les clés pour planifier le trajet le plus court possible passant au moins une fois par chacune des stations.

Le Tube Challenge n'est pas unique en son genre. Il s'agit d'une version plus compliquée d'un jeu joué dans la ville prussienne de Königsberg au XVIII^e siècle. Le fleuve Pregel se divise pour entourer l'île au cœur de la cité, puis les deux bras se rejoignent à l'ouest avant de se jeter dans la Baltique. Au XVIII^e siècle, il y avait sept ponts chevauchant la Pregel. Les promeneurs du dimanche avaient pour habitude de tenter de traverser tous les ponts une fois et une fois seulement avant de revenir au point de départ. À la différence du Tube Challenge, l'enjeu n'était pas de battre un record de vitesse mais tout simplement d'effectuer ce trajet selon les règles énoncées. Cependant, malgré leurs efforts, les promeneurs se rendaient compte qu'ils n'y arrivaient pas. Était-ce vraiment « mission impossible », ou bien existait-il un parcours qu'ils n'avaient

toujours pas effectué et qui leur permettrait de traverser les sept ponts ?

Le problème fut finalement résolu par Leonhard Euler, le mathématicien suisse qui avait posé le problème des carrés gréco-latins, alors qu'il enseignait à l'académie de Saint-Pétersbourg, à quelque 800 kilomètres au nord-est de Königsberg. Euler fit une avancée conceptuelle considérable. Il prit conscience que les dimensions physiques concrètes de la ville étaient sans importance : seule comptait la manière dont les ponts étaient liés les uns aux autres (principe qui régit également le plan topologique du métro londonien). Les quatre régions de terre reliées par les ponts de Königsberg peuvent chacune être réduites à un point, les ponts devenant alors des lignes reliant ces points. Cela donne une carte des ponts de Königsberg qui ressemble à un plan du métro de Londres mais beaucoup plus simple (figure 3.13).

Déterminer s'il est possible de parcourir une fois tous les ponts revient alors à vérifier s'il est possible de faire un tracé sur ce plan sans jamais lever le crayon ni repasser sur un trait. Grâce à ce nouveau point de vue mathématique, Euler conclut qu'il était en fait impossible de traverser la totalité des sept ponts une seule fois.

Mais pourquoi est-ce impossible ? Lorsque vous tracez votre chemin sur le plan, vous constatez que chaque point visité doit être associé à une ligne entrante et à une ligne sortante. Si vous deviez visiter à nouveau ce point, il faudrait emprunter un nouveau « pont » à l'aller, et encore un autre « pont » pour le retour. Par conséquent, chaque point doit être desservi par un nombre pair de lignes reliant les points, sauf en début et en fin de parcours.

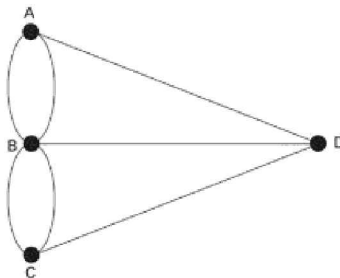


Fig. 3.13

Or, si nous regardons le plan des sept ponts de Königsberg, nous voyons que les quatre points sont desservis par un nombre impair de ponts : cela confirme qu'il n'y a aucun chemin dans cette

ville permettant de traverser chacun de ces ponts une fois et une fois seulement. Mais Euler poussa son analyse encore plus loin. Si le plan comporte précisément deux points desservis par un nombre impair de lignes, alors il devient possible de tracer le cheminement sans lever le crayon et sans passer une seconde fois sur le trait ; mais, pour ce faire, le point de départ et la destination doivent obligatoirement être, l'un et l'autre, un de ces deux points desservis par un nombre impair de lignes.

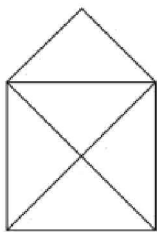


Fig. 3.14 Le théorème d'Euler implique qu'il est possible de dessiner ce schéma sans lever le crayon ni passer deux fois sur une même ligne.

Il existe une autre sorte de plan sur lequel il est possible de parcourir ce que les mathématiciens appellent un circuit eulérien, c'est-à-dire un parcours où tous les points sont desservis par un nombre pair de lignes. Sur un tel plan, vous pouvez démarrer où vous voulez, mais le parcours doit commencer et finir au même point afin de dessiner une boucle fermée. Même s'il n'est pas facile d'entrevoir le parcours, le théorème d'Euler nous indique que, tant que le plan appartient aux deux catégories que j'ai décrites, il doit y avoir soit un chemin eulérien, soit un circuit (partant et revenant au même point) eulérien. C'est toute la force des mathématiques : elles vous prouvent souvent que quelque chose existe sans que vous ayez besoin de le construire.

Afin de démontrer qu'un tel circuit existe, nous faisons usage d'une vieille arme de l'arsenal du mathématicien : l'induction. J'utilise quant à moi la même arme lorsqu'il s'agit de surmonter ma peur des hauteurs, si je dois par exemple grimper à une haute échelle ou descendre en rappel une chute d'eau : je procède par étapes.

Commencez par imaginer que vous savez tracer tous les plans ayant un certain nombre d'arêtes sans lever votre crayon de la feuille. Maintenant, vous vous trouvez face à un plan qui présente

une arête de plus que tous les plans vus jusqu'à présent. Comment déterminer s'il est possible de tracer également ce nouveau plan ?

Disons qu'il s'agit d'un plan composé de deux points — que nous appellerons point A et point B — d'où part un nombre impair d'arêtes. L'astuce consiste à retirer une arête d'un des points ayant un nombre impair d'arêtes. Donc, enlevons l'arête qui va du point B à un autre point, disons C. Ce nouveau plan se compose toujours de seulement deux points avec un nombre impair d'arêtes qui en sortent : A et C. (B a désormais un nombre d'arêtes pair puisque nous lui avons enlevé une arête, et C a maintenant un nombre impair d'arêtes car nous venons de lui enlever la ligne qui le reliait à B.) D'après l'hypothèse d'induction, il existe un chemin qui commence à A et finit à C et passe par toutes les arêtes de ce nouveau plan. L'autre plan, plus grand, est facile à dessiner : il suffit de relier C à B en ajoutant l'arête que nous avons retirée plus tôt. Et voilà !

Il y a quelques variations qu'il faudrait cependant analyser. Par exemple, que se passe-t-il s'il n'y a qu'une seule ligne qui va de B à A, et donc que A et C sont le même point ? Mais nous pouvons voir qu'au cœur de la démonstration d'Euler, il y a cette magnifique idée de construire étape par étape le chemin eulérien. Ainsi, cette même astuce qui me permet de gravir une échelle lentement mais sûrement me permet de trouver mon chemin dans un plan, si grand soit-il.

Pour voir la puissance du théorème d'Euler, mettez un ami au défi de tracer un plan aussi compliqué qu'il le souhaite. Puis, simplement en comptant le nombre de points où se rejoignent un nombre impair de lignes, grâce au théorème d'Euler, vous pouvez savoir immédiatement si le plan peut être dessiné en entier sans lever le crayon ou repasser sur une même ligne.

J'ai récemment fait un pèlerinage à Königsberg, rebaptisée Kaliningrad après la Seconde Guerre mondiale. En grande partie détruite par les bombardements alliés, la ville ne ressemble plus à celle que connut Euler. Trois des ponts subsistent cependant : le Holzbrücke, le Honigbrücke et le Hohe Brücke. En revanche, le Küttelbrücke et le Schmiedebrücke n'existent plus, et les deux derniers ponts — le Grüne Brücke et le Krämerbrücke —, également détruits pendant la guerre, ont été remplacés par une immense voie express qui traverse la ville.

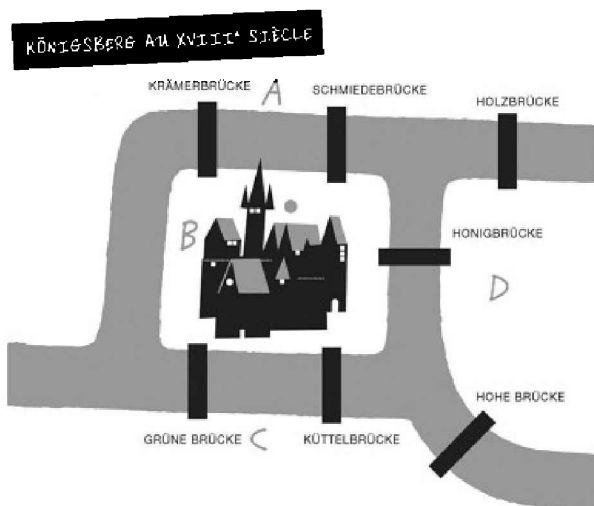


Fig. 3.15 Les ponts de Königsberg au XVIII^e siècle.

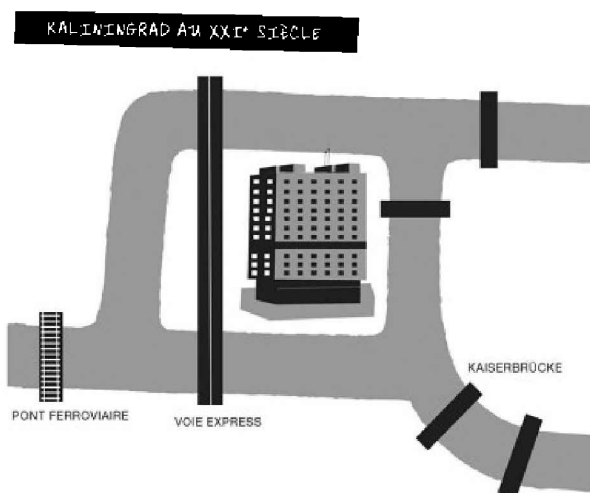


Fig. 3.16 Les ponts de Kaliningrad au XXI^e siècle.

Un nouveau pont ferroviaire, que les piétons peuvent également emprunter, relie maintenant les deux rives du Pregel à l'ouest de la ville ; et une passerelle baptisée Kaiserbrücke me permet d'effectuer la même traversée qu'autrefois le Hohe Brücke. Mathématicien dans l'âme, je me suis immédiatement demandé si un parcours dans l'esprit du jeu du XVIII^e siècle était possible via les ponts actuels.

Je savais, d'après les analyses mathématiques d'Euler, que s'il y avait exactement deux endroits desservis par un nombre impair de ponts, alors un chemin eulérien était possible. Il suffit de commencer à un des endroits comptant un nombre impair de ponts et de terminer à l'autre. En regardant le plan actuel de Kaliningrad, je compris qu'un tel parcours était en fait possible.

Si l'histoire des ponts de Königsberg est considérée comme importante, c'est qu'elle offrait aux mathématiciens une autre manière d'aborder la géométrie et l'espace. Au lieu de s'attacher aux distances et aux angles, cette nouvelle perspective ne s'intéressait qu'à la manière dont les formes sont reliées entre elles. Ainsi naquit la topologie, une des branches les plus importantes des mathématiques, étudiée depuis maintenant une centaine d'années, et sujet que nous avons abordé dans le chapitre 2. Le problème posé par les ponts de Königsberg a engendré le genre de mathématiques qui est aujourd'hui au cœur du fonctionnement des moteurs de recherche sur Internet, comme celui de Google, qui s'efforcent de maximiser les modes de navigation sur les réseaux. Et le point de vue d'Euler peut vous aider à parcourir le métro londonien et vous confronter au Tube Challenge.

COMMENT LA PREMIER LEAGUE PEUT VOUS FAIRE GAGNER UN MILLION MATHÉMATIQUE

En milieu de saison, votre équipe de foot se languit dans la seconde moitié du tableau, et vous voulez savoir si elle a encore une chance de remporter le championnat. Étonnamment, les mathématiques qui permettent de tenter de répondre à cette question sont directement liées au problème à un million de dollars posé dans ce chapitre.

Pour déterminer si mathématiquement c'est possible, vous partez de l'hypothèse que votre équipe remportera tous les matchs qui restent à jouer, ce qui vous donne trois points par match. La difficulté commence lorsqu'il faut distribuer le reste des points aux autres équipes. Il faut que les équipes au-dessus de vous perdent suffisamment de matchs pour que la vôtre les dépasse. Mais vous ne pouvez pas toutes les faire perdre, car ces équipes vont s'affronter entre elles, donc vous devez trouver le moyen de

distribuer les points entre les rencontres restantes et espérer qu'une combinaison vous permettra de demeurer en tête. Il doit sûrement exister un moyen plus astucieux pour savoir si une telle combinaison gagnante existe.

Ce qu'il vous faut, c'est une astuce semblable à celle utilisée par Euler pour tracer des circuits, et qui vous évite donc de passer en revue tous les scénarios de résultat possibles. Malheureusement, aujourd'hui nous ne savons pas si une telle astuce existe. Un million de dollars sera offert à quiconque trouvera cette astuce ou parviendra à prouver que seule une analyse exhaustive de tous les scénarios peut résoudre un problème aussi complexe.

Avant 1981, il existait cependant un programme efficace pour vérifier, en milieu de saison par exemple, si votre équipe pouvait encore espérer remporter le championnat. En effet, avant cette date, on n'attribuait que deux points par victoire, et un point par match nul. Mathématiquement, ce règlement avait son importance, car cela signifiait que le nombre total de points joués chaque saison était fixe. Par exemple, dans un championnat composé de 20 équipes comme la Premier League, chaque équipe jouait 38 matchs (à domicile et à l'extérieur contre les 19 autres équipes). Cela fait 20×38 matchs... sauf que j'ai compté chaque match deux fois. Les matchs d'Arsenal contre Manchester United, par exemple, sont les mêmes que ceux de Manchester United contre Arsenal. Donc, cela fait en réalité 10×38 , soit 380 matchs au total. Avec cet ancien système de points, le nombre total à la fin de la saison est $2 \times 380 = 760$, à répartir entre les 20 équipes. C'était là la clé d'un programme informatique efficace utilisé pour vérifier à mi-saison si votre équipe avait encore une chance ou non de remporter le titre.

D'un point de vue mathématique, tout changea en 1981, lorsqu'il fut décidé de donner trois points en cas de victoire et deux points en cas de match nul (un point par équipe) ; désormais, il est impossible d'anticiper le total de points à la fin de la saison. Si toutes les rencontres se soldent par des matchs nuls, le total des points est à nouveau 760, mais s'il n'y a aucun match nul, le total s'élève à 1 140 et c'est ce changement qui a rendu le problème de la Premier League si difficile à démêler.

Il existe de nombreuses variantes de ce problème qui n'ont rien à voir avec le foot. Un classique du genre est connu sous le nom de problème du représentant de commerce. Par exemple, un VRP doit rendre visite à 11 clients, chacun situé dans une ville différente. Ces localités sont reliées entre elles par des routes (voir le plan de la

figure 3.17). Or, notre voyageur de commerce n'a assez d'essence que pour effectuer au maximum 238 kilomètres.

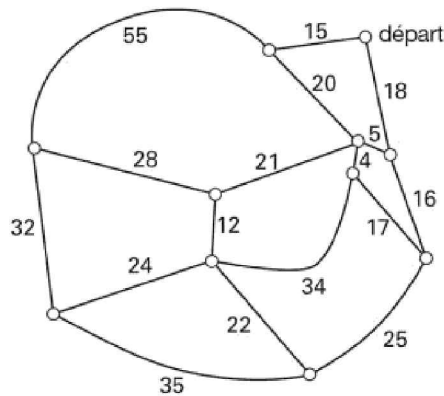


Fig. 3.17 Un exemple du problème du représentant de commerce.
Pouvez-vous trouver un parcours de 238 kilomètres maximum passant par tous les points et se terminant au point de départ ?

La distance entre les villes est indiquée sur chaque route les reliant. Pouvez-vous identifier le trajet permettant au voyageur de commerce de rendre visite aux 11 clients puis de rentrer chez lui sans tomber en panne d'essence ? (La solution est donnée en fin de chapitre.) Dans cette version du problème, le million de dollars ira à la personne qui saura trouver un algorithme général ou un programme informatique capable de déterminer le circuit le plus court — quel que soit le plan soumis à l'analyse du programme — de manière essentiellement plus rapide que par l'analyse exhaustive de tous les scénarios possibles par un ordinateur. Le nombre de parcours possibles croissant exponentiellement en fonction du nombre de villes, une analyse exhaustive devient vite impossible. Peut-on prouver qu'un algorithme général n'existe pas ?

La plupart des mathématiciens estiment que les problèmes de ce genre ont une complexité inhérente, c'est-à-dire qu'aucune astuce ne fournira de solution. Je les appelle les problèmes « aiguille dans une botte de foin » car il y a un grand nombre de solutions possibles et qu'il s'agit d'en trouver une particulière. Le nom technique de ce type de problèmes est « problème NP-complet ».

Une des caractéristiques de ces casse-tête est qu'une fois qu'on a trouvé l'aiguille, il est facile de vérifier qu'elle fait l'affaire. Par exemple, dès qu'on a trouvé un parcours sur le plan inférieur à

238 kilomètres, on le vérifie trivialement. De la même manière, si on parvient à la bonne combinaison de résultats pour le reste de la saison de foot, on sait tout de suite si notre équipe a encore une chance mathématique de remporter le titre de champion. Un problème P est un problème pour lequel il existe un programme efficace capable de trouver la solution. La question à un million de dollars peut être énoncée ainsi : les problèmes NP-complets sont-ils en fait des problèmes P ? Les mathématiciens la formulent, quant à eux, ainsi : $NP \leq P$.

Tous ces problèmes NP-complets ont en commun une propriété très curieuse. Si on a un programme efficace qui fonctionne pour un problème, il y aura aussi un tel programme pour tous les autres problèmes. Par exemple, si on trouve un programme astucieux capable d'indiquer au représentant de commerce le chemin le plus court, il peut également être efficace pour vérifier si votre équipe a encore des chances de remporter le championnat. Pour donner une idée d'un tel fonctionnement, voici deux autres problèmes NP-complets aux allures très différentes.

Le problème des soirées diplomatiques

Vous prévoyez d'organiser une soirée à laquelle vous souhaitez inviter vos amis, mais certains d'entre eux se détestent, et comme vous ne voulez pas que deux personnes en conflit se croisent, vous décidez d'organiser trois soirées et d'y inviter des gens différents. Est-il possible d'envoyer des invitations de telle manière qu'il n'y ait pas deux ennemis à la même soirée ?

Le problème de la carte tricolore

Dans le chapitre 2, nous avons vu qu'il ne faut que quatre couleurs pour colorer une carte. Mais existe-t-il un moyen efficace de déterminer s'il serait possible de colorer n'importe quelle carte avec seulement trois couleurs ?

Comment une solution au problème de la carte tricolore peut-elle nous aider à résoudre le problème des soirées diplomatiques ? Regardez ce qui se passe si, après avoir inscrit les prénoms de vos amis, vous reliez ceux qui se détestent.

Le problème des soirées diplomatiques et celui de la carte tricolore sont des versions différentes de la même question, donc si on trouve une manière efficace de résoudre un seul problème NP-complet, alors on trouve comment les résoudre tous ! Voici une sélection de problèmes, vous pouvez essayer avec l'un d'entre eux — convenablement généralisé — de gagner un million de dollars.

Le démineur

Ce jeu sur ordinateur pour un joueur est systématiquement fourni avec le système d'exploitation Microsoft. Le but du démineur est de déterminer l'emplacement de mines sur une grille afin de les éviter. Si on clique sur un carré dans la grille et qu'aucune mine ne s'y trouve, le jeu indique alors combien de carrés mitoyens contiennent, eux, des mines. En revanche, si on clique sur un carré contenant une mine, on est mort. Le défi du démineur, d'une valeur d'un million de dollars, est un peu différent. L'image suivante est, par exemple, impossible dans le jeu habituel puisque aucune disposition de mines n'est capable d'engendrer ces chiffres (figure 3.20). En effet, le 1 implique qu'un des deux carrés mitoyens non encore dévoilés contient une mine, alors que le 2 indique que ces deux mêmes carrés en contiennent. Mais que dire de l'image suivante (figure 3.21) : pourrait-elle provenir d'un vrai jeu ?

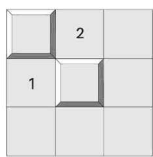


Fig. 3.20

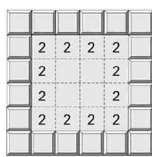


Fig. 3.21

Peut-on placer des mines de manière à donner raison aux chiffres ? Ou est-il impossible qu'elle provienne d'un vrai jeu car il n'y a aucune disposition de mines permettant les nombres indiqués ? Votre tâche consiste à élaborer un programme efficace qui résoudra ce problème quelle que soit l'image que l'on vous soumette.

Sudoku

Trouver un programme efficace pour résoudre des sudokus arbitrairement grands est un problème NP-complet. Parfois, lorsqu'il s'agit de sudokus difficiles, il vous faut émettre des suppositions puis poursuivre en fonction des implications logiques qu'elles engendrent ; il ne semble pas exister de moyen de deviner astucieusement, il faut essayer des séries de suppositions jusqu'à ce que l'une d'entre elles vous oriente vers une réponse satisfaisante.

Le problème de l'empilement

Vous êtes l'heureux propriétaire d'une entreprise de déménagement. Tous vos cartons sont de même hauteur et de même largeur, et leur taille correspond aux dimensions intérieures de votre wagon (juste un peu moins pour pouvoir les y glisser). Or, les longueurs des cartons sont variables. Sachant que le camion fait 150 pieds de long et que vos cartons font les longueurs suivantes : 16, 27, 37, 42, 52, 59, 65 et 95 pieds, pouvez-vous agencer les cartons de manière à optimiser la contenance du wagon ? Pour ce faire, vous devez trouver un algorithme qui détermine, pour tout nombre N et toute série de nombres plus petits $n(1), n(2), \dots, n(r)$, s'il existe un choix de nombres plus petits dont la somme est égale à N .

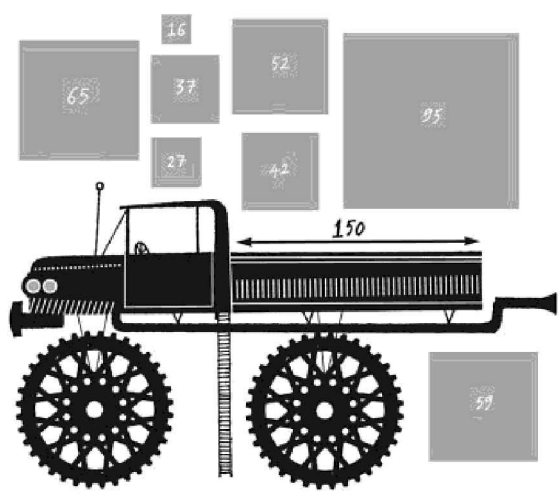


Fig. 3.22 Empiler des cartons est un problème mathématiquement complexe.

Des problèmes de ce type ne sont pas que des jeux : ils surgissent dans le monde des affaires et de l'industrie lorsque des entreprises doivent trouver des solutions efficaces à un problème d'ordre pratique. Un espace mal optimisé ou des dépenses excessives en carburant coûtent de l'argent aux sociétés, et les gestionnaires ont souvent besoin de résoudre de tels problèmes NP. Ainsi, il n'y a pas que les mathématiciens et les joueurs obsessionnels qui cherchent à « cracker » ce problème à un million de dollars.

Qu'il s'agisse d'analyser mathématiquement des championnats de foot ou d'organiser des soirées par affinités, de colorier des cartes ou de déterminer l'emplacement de mines, le problème à un million de dollars de ce chapitre revêt tant de formes différentes qu'il doit sûrement exister au moins une version à votre goût. Mais soyez prévenu : en dépit de son allure ludique, il s'agit d'un des problèmes à un million de dollars les plus difficiles de tous. Les mathématiciens pensent que ces problèmes sont d'une telle complexité qu'aucun programme informatique ne parviendra à les résoudre. Or, il est toujours bien plus difficile de démontrer que quelque chose *n'existe pas* que de démontrer qu'il existe. Mais au moins, vous pouvez vous amuser en essayant de gagner le million de ce chapitre.

SOLUTIONS

Les six bons numéros de la loterie

Les numéros gagnants sont les 2 3 5 7 17 42.

Le problème du représentant de commerce

Voici un trajet qui fait 238 kilomètres :

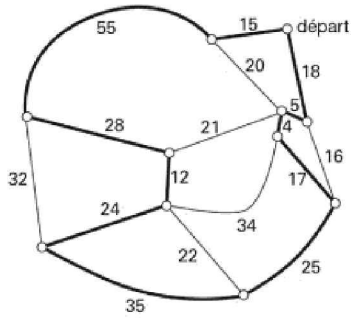


Fig. 3.23

$$15 + 55 + 28 + 12 + 24 + 35 + 25 + 17 + 4 + 5 + 18 = 238$$

Chapitre IV

LE CAS DU CODE INCASSABLE

Depuis que les hommes ont appris à communiquer, ils n'ont eu de cesse de trouver des moyens plus diaboliques les uns que les autres pour cacher des messages à leurs ennemis. Peut-être utilisiez-vous un code pour rédiger votre journal intime afin que votre frère ou votre sœur ne puisse le lire, à la manière de Léonard de Vinci. Mais les codes ne servent pas uniquement à cela : ils garantissent aussi la diffusion sans erreur d'une information. Grâce aux mathématiques, il est possible de concevoir des méthodes ingénieuses pour s'assurer que le message reçu est identique à celui qui a été envoyé — principe d'une importance capitale en cette ère de transactions électroniques.

Un code est simplement une manière systématique pour agencer une série de symboles afin de transmettre un message particulier. En y regardant de plus près, on découvre que les codes sont partout : il y a des codes-barres sur tout ce que nous achetons ; des codes nous permettent de stocker de la musique sur nos lecteurs MP3 ; et c'est grâce aux codes que nous pouvons naviguer sur Internet. Même ce livre est écrit dans un code — la langue est simplement un code composé des 26 lettres de l'alphabet, et nos « mots de code acceptables » sont stockés dans nos dictionnaires. Même nos corps contiennent des codes : l'ADN est un code pour reproduire une créature vivante composé de quatre substances chimiques organiques appelées des bases : adénine, guanine, cytosine et thymine, ou A, G, C et T.

Dans ce chapitre, je vous montrerai comment les mathématiques ont été utilisées pour créer et déchiffrer certains des codes les plus ingénieux qui soient, et comment ces codes nous permettent non seulement de transmettre des informations de manière sûre, efficace et secrète, mais aussi de faire toutes sortes de choses, de la photographie des planètes depuis une navette spatiale à des achats sur eBay. Et, à la fin du chapitre, je vous

expliquerai comment la résolution d'un des problèmes à un million de dollars pourrait également vous aider à casser certains codes.

COMMENT UTILISER UN ŒUF POUR ENVOYER UN MESSAGE SECRET

En Italie, au XVI^e siècle, Giovanni Porta découvrit qu'il était possible d'écrire un message « invisible » sur un œuf dur grâce à de l'encre fabriquée à partir d'une once d'alun mélangée à une pinte de vinaigre. L'encre pénètre la coquille et teinte le blanc à l'intérieur mais, tandis que l'encre reste sur le blanc, elle disparaît de la surface de la coquille. Parfait pour envoyer des messages secrets — pour casser le code, il suffit de casser l'œuf ! Et cela n'est qu'une des nombreuses façons farfelues de cacher des messages secrets.

En 499 av. J.-C., un tyran du nom d'Histiée voulut envoyer un message secret à son neveu Aristagoras pour l'inciter à se révolter contre le roi perse Darius I^{er}. Histiée était retenu à Suse, dans l'Iran actuel, tandis que son neveu était chez eux à Milet, aujourd'hui en Turquie. Comment faire pour transmettre un message à son neveu sans qu'il soit intercepté par les autorités perses ? Une ruse lui vint à l'esprit. Il rasa la tête de son plus fidèle esclave et tatoua le message sur son crâne. Une fois que les cheveux eurent repoussé, Histiée envoya l'esclave rejoindre son neveu, lequel rasa la tête du messenger pour y découvrir le message et lancer la révolte contre le roi.

Tandis que le neveu n'avait qu'à raser la tête du messenger pour obtenir le message, les destinataires des messages secrets envoyés à l'époque de la Chine ancienne étaient plus à plaindre. Le message était écrit sur un morceau de soie qui, après avoir été enroulé très serré et enduit de cire, devait être avalé. Récupérer le message à sa sortie n'était pas une affaire plaisante.

Une des manières les plus sophistiquées de cacher un message fut élaborée par les Spartiates en 500 av. J.-C. Ils utilisaient un cylindre en bois spécial appelé une scytale qu'ils entouraient de bas en haut d'une fine lanière de parchemin. Le message secret était alors inscrit sur le parchemin, dans le sens de la longueur de la scytale. Lorsque la lanière était retirée du cylindre, le message devenait illisible. Ce n'est qu'en enroulant à nouveau la lanière sur

une autre scytale exactement de même diamètre que les lettres s'alignaient correctement.

Ces méthodes pour envoyer des messages secrets sont davantage des exemples de stéganographie — l'art de dissimuler — que de codage. Mais si rusées fussent-elles, une fois que le message était découvert, le secret était révélé. Ainsi, les gens ont commencé à réfléchir à un moyen de dissimuler le sens du message même si ce dernier venait à être découvert.

COMMENT DÉCHIFFRER LES CODES DU KAMASUTRA EN COMPTANT

B OBDFSOBDLNLBC, ILXS B QBLCDSV MV B QMSD, LE B
OBXSV MH QBDDSVCE.

LH FLE QBDDSVCE BVS OMVS QSVBCSCD DFBC DFSLVE,
LD LE ASNBGES DFSJ BVS OBTS ZLDF LTSBE. DFS
OBDFSOBDLNLBC'E QBDDSVCE, ILXS DFS QBLCDSV'E MV
DFS QMSD'E OGED AS ASBGDLHGI ; DFS LTSBE ILXS DFS
NMIMGVE MV DFS ZMVTE, OGED HLD DMUSDFSV LC B
FBVOMCLMGE ZBJ. ASBGDJ LE DFS HLVED DSED : DFSVS LE
CM QSVBCSCD QIBNS LC DFS ZMVIT H MV GUIJ
OBDFSOBDLNE.

On dirait du charabia, mais c'est un message écrit à l'aide d'un des codes les plus populaires jamais créés. Appelé le chiffrement par substitution, ce code fonctionne sur la substitution de chaque lettre de l'alphabet par une autre : ainsi un « a » peut devenir un « P », « t » peut devenir « C », et ainsi de suite. (J'utilise des minuscules pour le message non crypté, le texte clair, et des majuscules pour les lettres du message chiffré.) À condition que l'envoyeur et le destinataire se soient mis d'accord en amont sur la clé de déchiffrement, le destinataire pourra déchiffrer le message, mais pour toutes les autres personnes, il n'aura aucun sens.

La version la plus simple de ces codes s'appelle les « chiffres de César » — car Jules César utilisa ce procédé pour communiquer avec ses généraux durant la guerre des Gaules. Le principe consiste à substituer à chaque lettre du message celle qui se trouve à un certain rang plus loin dans l'alphabet. Ainsi, si l'on choisit un décalage de trois lettres, « a » devient « D », « b » « E », etc. Depuis

la page Web de ce livre, vous pouvez télécharger et découper votre propre roue de chiffrement afin de créer ces simples « chiffres de César ».

Remplacer chaque lettre par une autre lettre à distance fixe ne vous donne que 25 clés possibles, donc, dès que vous avez compris que c'est ainsi que le message a été codé, il devient assez aisé de le déchiffrer. Il existe un encore meilleur moyen de chiffrer : au lieu de procéder à ce décalage systématique, on peut remplacer une lettre par n'importe quelle autre lettre. Cette méthode fut en réalité suggérée plusieurs siècles avant Jules César, non pas dans un manuel militaire mais, curieusement, dans le *Kamasutra*.

Bien que ce texte ancien écrit en sanskrit soit généralement associé à la description des plaisirs physiques, il traite de quantité d'autres arts qu'une femme se devait de connaître, de la prestidigitation aux échecs en passant par la reliure de livres et la menuiserie. Le 45^e chapitre, consacré à l'art de l'écriture secrète, décrit le chiffrement par substitution comme un moyen parfaitement adapté pour communiquer discrètement entre amants.

Un chiffre de César n'a que 25 clés. Or, si nous nous permettons de remplacer n'importe quelle lettre par n'importe quelle autre lettre, alors le nombre de chiffrements possibles est bien plus grand. Nous avons 26 choix pour modifier la lettre « a » et pour chacune de ces possibilités nous avons alors 25 choix pour la lettre « b » (une lettre a déjà été utilisée pour encoder la lettre « a »). Donc il y a déjà 26×25 différentes manières de chiffrer les lettres « a » et « b ». Si nous poursuivons ainsi, et que nous continuons d'attribuer différentes lettres au reste de l'alphabet, nous voyons qu'il y a :

$$\begin{aligned} &26 \times 25 \times 24 \times 23 \times 22 \times 21 \times 20 \times 19 \times 18 \times 17 \times 16 \times \\ &15 \times 14 \times 13 \times 12 \times 11 \times 10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times \\ &2 \times 1 \end{aligned}$$

différents chiffres. Comme nous l'avons vu page 71, nous pouvons écrire cela 26 !. Il faut également penser à retirer 1 à ce nombre car un des choix a consisté à remplacer « a » par « A », « b » par « B », etc., jusqu'à « z » par « Z », ce qui ne constitue pas un code très efficace ! Lorsque nous effectuons la multiplication de 26 !, et retirons 1, nous obtenons

chiffres différents — soit plus de quatre cents millions de milliards de milliards de possibilités.

Le passage qui figure en début du chapitre est chiffré de cette manière. Pour vous donner une idée de ce nombre de permutations, si nous devions écrire le passage en utilisant tous les codes possibles, la feuille de papier s'étendrait d'ici jusqu'à bien au-delà des abords de notre Voie lactée. Un ordinateur capable de vérifier chaque code en une seconde, et ce depuis le Big Bang il y a plus de 13 milliards d'années, n'aurait effectué qu'une fraction de la tâche consistant à vérifier chacun des codes — une toute petite fraction qui plus est.

Ce message semble donc indéchiffrable : comment identifier le code parmi tant de codes possibles ? En réalité, chose étonnante, c'est tout à fait faisable, il suffit de compter.

	a	b	c	d	e	f	g	h	i	j	k	l	m
%	8	2	3	4	13	2	2	6	7	0	1	4	2
	n	o	p	q	r	s	t	u	v	w	x	y	z
%	7	8	2	0	6	6	9	3	1	2	0	2	0

Table 4.01 La fréquence de répartition des lettres dans la langue anglaise, à 1 % près. Grâce à cette information il est possible de commencer à décoder des messages chiffrés par substitution.

Ce sont les Arabes à l'époque de la dynastie des Abbassides qui, les premiers, mirent au point la cryptanalyse, la science du déchiffrement. Yaqub al-Kindi, un savant du IX^e siècle, observa que dans un extrait de texte, des lettres reviennent souvent tandis que d'autres sont rarement utilisées, comme le montre la table 4.01. C'est un phénomène avec lequel les joueurs de Scrabble sont familiers. Dans le jeu, la lettre E ne vaut qu'un point car c'est la lettre la plus courante du français, tandis que la lettre Z, plus rare, vaut 10. Dans un texte écrit, chaque lettre a sa propre « personnalité » — c'est-à-dire sa propre fréquence d'apparition et sa manière de se combiner à d'autres lettres —, mais le point clé de l'analyse d'Al-Kindi c'est d'avoir mis en évidence que la « personnalité » d'une lettre ne change pas lorsque celle-ci est représentée par un autre symbole. Tentons donc de déchiffrer le texte en début de partie.

	A	B	C	D	E	F	G	H	I	J	K	L	M
%	1	10	5	12	7	6	3	2	2	1	0	8	5
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
%	2	4	0	3	0	13	1	1	7	0	1	0	1

Table 4.02 La fréquence de répartition des lettres dans le texte chiffré.

La table 4.02 donne la fréquence des lettres employées dans le texte chiffré. On peut voir que la lettre « S » a une fréquence de 13 %, plus que toutes les autres lettres du texte chiffré, il est donc fort probable que c’est la lettre utilisée pour chiffrer la lettre « e ». (Bien évidemment, il ne vous reste plus qu’à espérer que je n’ai pas choisi un passage du roman *La Disparition* de Georges Perec, écrit sans un seul « e ».)

La deuxième lettre la plus courante dans le texte est « D », avec une fréquence de 12 %. En anglais, la deuxième lettre la plus courante est la lettre « t », donc on peut supposer que « D » représente « t ». Le « B » a quant à lui une fréquence de 10 %, on peut donc tenter de le remplacer par la troisième lettre la plus courante de la langue anglaise, le « a ».

Procédons à une première étape de substitutions afin de voir ce que cela donne :

a OatFeOatLNLaC, ILXe a QaLCteV MV a QMet, LE a OaXeV MH QatteVCE.

LH FLE QatteVCE aVe OMVe QeVOaCeCt tFaC tFeLVE, Lt LE AeNaGEe tFeJ aVe OaTe ZLtF LTeaE. tFe OatFeOatLNLaC'E QatteVCE, ILXe tFe QaLCteV'E MV tFe QMet'E OGEt Ae AeaGtLHGI ; tFe LTeaE ILXe tFe NMIMGVE MV tFe ZMVTE, OGEt HLt tMUetFeV LC a FaVOMCLMGE ZaJ. AeaGtJ LE tFe HLVEt teEt : tFeVe LE CM QeVOaCeCt QIaNe LC tFe ZMVIT H MV GUIJ OatFeOatLNE.

Vous pensez sans doute que cela ressemble toujours à du charabia, mais le fait que la lettre « a » soit à plusieurs reprises toute seule nous indique que nous sommes sur la bonne voie (« a » en anglais est un article indéfini, notre « un » ou « une »). (Évidemment, il se peut que « B » soit en réalité un « i », auquel cas

il nous faudra reprendre depuis le début.) Le mot « tFe » revient souvent, donc on peut supposer qu'il s'agit du mot « *the* ». De plus, la lettre « F » a une fréquence de 6 % dans le texte chiffré, tout comme la lettre « h » dans la langue anglaise.

Dans le mot « Lt » seule la seconde lettre a été déchiffrée, or nous savons qu'il n'existe que deux mots en anglais composés de deux lettres et se finissant par un « t » : « *at* » (« à ») et « *it* » (« cela »). Comme nous avons déjà déchiffré le « a », alors il y a de grandes chances pour que « L » soit le « i », et notre tableau des fréquences confirme ce choix, « L » ayant une fréquence de 8 % dans notre texte et « i » de 7 % dans la langue anglaise, ce qui est suffisamment proche. La méthode que nous utilisons n'est pas une science exacte, et il faut savoir que plus un texte est long, plus les fréquences seront au diapason.

Procédons à présent au remplacement de ces deux lettres :

a OatheOatiNiaC, IiXe a QaiCteV MV a QMet, iE a OaXeV MH
QatteVCE.

iH hiE QatteVCE aVe OMVe QeVOaCeCt thaC theiVE, it iE
AeNaGEe theJ aVe OaTe Zith iTeaE. the OatheOatiNiaC'E
QatteVCE, IiXe the QaiCteV'E MV the QMet'E OGEt Ae
AeaGtiHGI ; the iTeaE IiXe the NMIMGVE MV the ZMVTE, OGEt
Hit tMUetheV iC a haVOMCiMGE ZaJ. AeaGtJ iE the HiVEt teEt :
theVe iE CM QeVOaCeCt QIaNe iC the ZMVIT HMV GUIJ
OatheOatiNE.

Progressivement, le message émerge. À vous maintenant de déchiffrer les autres lettres (le texte clair figure en fin de chapitre). Un indice cependant : il s'agit de deux de mes passages préférés du livre du mathématicien G. H. Hardy intitulé *L'Apologie d'un mathématicien*. C'est entre autres à la suite de la lecture de ce livre, quand j'étais élève, que j'ai décidé de devenir mathématicien.

Cette simple astuce mathématique consistant à compter la fréquence des lettres signifie que tout message déguisé grâce à un chiffre de substitution n'est pas véritablement secret — Marie Stuart reine d'Écosse l'apprit à ses dépens. Complotant d'assassiner la reine Élisabeth I^{re}, elle communiquait avec son complice Anthony Babington en utilisant un code où chaque lettre était remplacée par d'étranges symboles (figure 4.01).

A	B	C	D	E	F	G	H
○	⚡	Λ	≡	α	□	⊖	∞
I	K	L	M	N	O	P	Q
l	⊖	η		∅	▽	5	m
R	S	T	U	X	Y	Z	
f	Δ	ε	Ⓒ	7	8	9	

Fig. 4.01 Le code Babington.

À première vue, les messages qu’envoyait Marie semblaient impénétrables, mais Élisabeth s’était entourée d’un des plus grands casseurs de codes d’Europe, Thomas Phelippes. Ce n’était pas un bel homme, à en croire les écrits de l’époque il était petit, maigre, le cheveu couleur paille, la barbe jaune et clairsemée, le visage vérolé. Beaucoup de personnes étaient convaincues qu’il avait dû pactiser avec le diable pour être capable de lire de tels hiéroglyphes, mais son astuce reposait tout simplement sur ce même principe d’analyse fréquentielle. Il cassa le code, et Marie fut arrêtée. Les missives déchiffrées apportèrent la preuve des méfaits qu’elle complotait, à la suite de quoi elle fut jugée coupable et exécutée.

COMMENT LES MATHÉMATICIENS ONT-ILS CONTRIBUÉ À LA VICTOIRE DES ALLIÉS EN 1945 ?

Dès lors que la faiblesse inhérente aux codes par substitution fut établie, les cryptographes s’employèrent à trouver des techniques ingénieuses pour contrer des attaques fondées sur l’analyse fréquentielle. Une des idées consistait à varier le chiffre de substitution. Au lieu d’utiliser un seul chiffre de substitution pour chiffrer la totalité du texte, il est possible d’alterner entre deux chiffres. Ainsi, si vous souhaitiez chiffrer le mot *beef* (« bœuf »), alors chaque lettre « e » de ce mot serait chiffrée différemment, le premier « e » selon un chiffre, le second selon un autre ; ainsi « *beef* » pourrait très bien être chiffré pour donner *pork* (« porc »).

Plus on souhaite sécuriser un message, plus on applique de chiffres différents.

Bien sûr, il faut trouver le juste équilibre entre une plus grande sécurité et la maniabilité. Le plus sûr des chiffres, appelé un masque jetable, emploie un chiffre de substitution différent pour chacune des lettres d'un texte. Il est quasiment incassable car absolument rien n'indique par quel angle attaquer le texte. Et comme il faut trouver un chiffre de substitution différent pour chacune des lettres, il est très fastidieux.

Selon le diplomate français du XVI^e siècle Blaise de Vigenère, il suffisait, pour empêcher toute analyse fréquentielle, d'utiliser juste quelques chiffres de substitution. Bien que le chiffre de Vigenère, comme on l'appela, fût une forme d'encryptage puissante, il n'était pas incassable, et le mathématicien anglais Charles Babbage finit par trouver un moyen pour casser le code. Babbage est considéré comme le grand-père de l'informatique car il était convaincu que des machines pourraient être utilisées pour automatiser les calculs. C'est grâce à sa manière systématique d'aborder des problèmes qu'il eut, en 1854, l'idée lui permettant de casser le chiffre de Vigenère.

La méthode de Babbage repose sur l'un des principaux savoir-faire du mathématicien : la reconnaissance des formes. La première chose à repérer est le nombre de chiffres de substitution différents utilisés pour chiffrer le message. Comme l'article défini anglais « *the* » apparaîtra habituellement souvent dans n'importe quel texte clair, percevoir des répétitions de la même séquence de trois lettres peut constituer la clé pour découvrir combien de chiffres sont utilisés. Ainsi, par exemple, il est possible qu'on note que « AWR » apparaisse fréquemment, et qu'il y a toujours un intervalle composé d'un multiple de quatre lettres entre les occurrences de « AWR ». Ce serait là une bonne indication que quatre chiffres ont servi pour encoder le texte.

Muni de cette information, on divise le texte chiffré en quatre groupes. Le premier est constitué de la première, cinquième, neuvième lettre et ainsi de suite, le deuxième de la deuxième, sixième, dixième lettre et ainsi de suite. Le même chiffre de substitution ayant été utilisé pour coder les lettres dans n'importe lequel de ces quatre groupes, il est désormais possible d'analyser la fréquence dans chaque groupe, l'un après l'autre, et le code sera cassé.

Dès lors que le chiffre de Vigenère put être cassé, il fallut trouver une nouvelle manière de chiffrer des messages en toute

sécurité. Lorsque, dans les années 1920, la machine Enigma fut conçue en Allemagne, la plupart des gens pensaient qu'une méthode de chiffrement absolument inviolable avait enfin été trouvée.

Le principe d'Enigma est de changer le chiffre de substitution à chaque fois qu'une lettre est chiffrée. Si je veux chiffrer la séquence « aaaaaa » (pour signifier par exemple que j'ai mal), alors chaque « a » sera chiffré d'une manière différente. La beauté de cette machine est qu'elle opérait le changement d'une substitution à une autre de manière mécanique et très efficace. Le message était saisi sur un clavier. Au-dessus du clavier se trouve une seconde banque de lettres sous la forme d'un « tableau lumineux » ; lorsqu'une touche du clavier est enfoncée, une des lettres de ce tableau s'illumine pour indiquer la lettre chiffrée. Mais le clavier n'est pas branché directement à ce panneau lumineux : les connexions passent par un jeu de trois disques rotatifs reliés entre eux par un labyrinthe de câbles électriques.

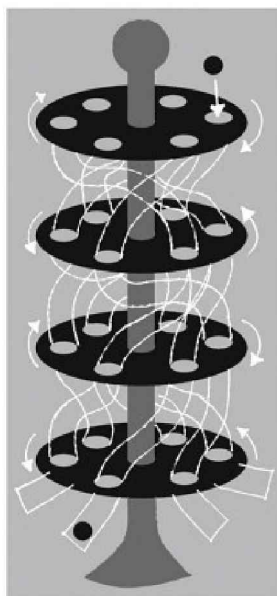


Fig. 4.02 Le principe de la machine Enigma : on fait tomber une boule dans les tubes pour chiffrer une lettre. Les tambours tournent à chaque nouvelle lettre afin de modifier, à chaque fois, le chiffrement.

Pour comprendre le fonctionnement d'Enigma, il suffit d'imaginer un large cylindre composé de trois tambours rotatifs.

En haut du cylindre se trouvent 26 trous, chacun étiqueté d'une lettre de l'alphabet. Pour chiffrer une lettre, on fait tomber une boule dans le trou correspondant à cette lettre. La boule tombe alors dans le premier tambour dont le haut et le bas sont également percés de 26 trous. Des tubes relient les trous supérieurs et inférieurs — mais ils ne relient pas le trou au-dessus avec celui situé directement en dessous. Au lieu de cela, les tubes s'entrelacent de manière qu'une boule entrant en haut du tambour sorte par un trou situé ailleurs en bas du tambour. Les tambours situés au milieu et en bas du cylindre fonctionnent sur le même principe ; mais leurs tubes internes relient les trous d'en haut et d'en bas de manières différentes. Lorsque la boule sort du trou en bas du troisième et dernier tambour, elle entre dans la dernière partie de l'engin et sort enfin par un des 26 trous situés en bas du cylindre, trous également étiquetés avec les lettres de l'alphabet.

Cela étant, si cette machine était restée telle quelle, il ne s'agirait que d'une manière compliquée de reproduire un chiffre de substitution. Mais voici le génie de la machine Enigma : chaque fois qu'une boule tombe dans le cylindre, le premier tambour effectue une rotation de $1/26^{\circ}$ de tour. Ainsi, lorsque la boule suivante sera introduite, le premier tambour lui fera emprunter un chemin complètement différent. Par exemple, si la lettre « a » est chiffrée disons en « C » par cette machine, dès que le tambour effectue un premier mouvement de rotation, une balle placée dans le trou « a » sortira d'un tout autre trou en bas. Il en allait de même avec Enigma : une fois que la première lettre avait été chiffrée, le premier disque rotatif (ou rotor) avançait d'un cran.

Les disques rotatifs fonctionnent un peu comme un compteur kilométrique : une fois que le premier disque a effectué un tour complet (les 26 crans) et qu'il revient à sa position de départ, cela enclenche la rotation du second disque de $1/26$ de tour. Donc en tout il y a $26 \times 26 \times 26$ différentes manières de chiffrer les lettres. En outre, l'opérateur de la machine avait la possibilité de modifier l'ordre des disques, ce qui multipliait le nombre de chiffres de substitution possibles par un facteur 6 (ce qui correspond aux 3 ! différentes manières d'agencer les trois disques).

Chaque chiffrer recevait quotidiennement des instructions indiquant la position initiale des trois disques. Le destinataire déchiffrait le message à l'aide des mêmes instructions de réglage. On complexifia encore Enigma au fil du temps jusqu'à obtenir 158 trillions de combinaisons différentes de réglages initiaux possibles.

En 1931, le gouvernement français fit la découverte des plans de la machine allemande et il fut horrifié. Apparemment, il n’y avait aucun moyen de déterminer, à partir d’un message intercepté, comment les disques avaient été réglés pour le chiffre du jour — ce qui était crucial si on voulait déchiffrer le message. Cependant, la France avait signé un accord d’échange de renseignements avec les Polonais, et la menace d’une invasion allemande eut pour effet d’inciter ces derniers à se mettre d’urgence au travail de décryptage.

Les mathématiciens en Pologne notèrent que chaque réglage des disques avait des caractéristiques propres, et qu’il était donc possible d’exploiter la présence de régularités pour faire un travail à rebours et décoder des messages. Si le chiffreur saisissait un « a » par exemple, cette lettre était alors chiffrée en fonction du réglage des disques et donnait disons un « D ». Le premier disque passait alors au cran suivant. Lorsqu’un autre « a » était ensuite tapé, il était peut-être chiffré en un « Z », donc, d’une certaine façon, « D » était lié à « Z » par la manière dont les disques avaient été réglés.

Regardons cela de plus près grâce à notre machine à tambours. En réinitialisant les tambours et en faisant tomber des boules deux fois à travers chacune des lettres, nous pouvons élaborer une série complète de relations ayant cette allure (table 4.03).

Lettre à coder	a	b	c	d	e	f	g	h	i	j
1 ^{re} boule	D	T	E	R	F	A	Q	Y	S	I
2 ^e boule	Z	S	B	Q	X	G	L	V	K	A
Lettre à coder	k	l	m	n	o	p	q	r	s	t
1 ^{re} boule	P	B	N	C	G	Z	J	H	M	U
2 ^e boule	J	D	Y	H	C	W	E	O	I	M
Lettre à coder	v	w	x	y	z					
1 ^{re} boule	K	O	W	L	V					
2 ^e boule	P	F	N	R	U					

Table 4.03

Sur www.4thestate.co.uk/2012/08/numbermysteries/, il est possible de télécharger un mode d'emploi au format PDF pour fabriquer sa propre machine Enigma.

Chaque lettre apparaît une fois et une fois seulement dans chaque rangée car chaque rangée correspond à un seul code de substitution.

Comment les Polonais exploitèrent-ils ces relations ? Les chiffreurs d'Enigma utilisaient tous un même réglage chaque jour. Ensuite, ils choisissaient chacun leur propre réglage, qu'ils envoyaient dans un message chiffré selon le premier réglage. Pour garantir un maximum de sécurité, on leur demandait de répéter leur choix pour ce nouveau réglage en le tapant deux fois. Loin d'être sûr, ce procédé fut au contraire une erreur fatale. Cela donna aux Polonais un début d'information concernant la relation des disques et des lettres, autrement dit le réglage du jour de la machine Enigma.

Des mathématiciens basés dans une maison de campagne à Bletchley Park, à mi-chemin entre Oxford et Cambridge, étudièrent les régularités mises en évidence par leurs collègues polonais et trouvèrent le moyen d'automatiser la recherche des réglages grâce à une machine de leur cru qu'ils appelaient une « bombe ». On a dit que ces mathématiciens ont raccourci la Seconde Guerre mondiale de deux ans, et ont par conséquent contribué à sauver d'innombrables vies. En outre, leurs machines sont à l'origine des ordinateurs que nous utilisons aujourd'hui.

FAIRE PASSER LE MESSAGE

Qu'un message soit chiffré ou non, il faut trouver un moyen de l'acheminer d'un lieu à un autre. De nombreuses civilisations anciennes, des Chinois aux Indiens d'Amérique, utilisaient des signaux de fumée pour communiquer sur de grandes distances. On dit que les feux allumés sur les tourelles de la Grande Muraille de Chine pouvaient communiquer un message sur 500 kilomètres le long de la Muraille en seulement quelques heures.

Les codes visuels fondés sur l'utilisation de drapeaux remontent à 1684, lorsque Robert Hooke, un des plus célèbres savants du XVII^e siècle, proposa l'idée à la Royal Society à Londres. L'invention du télescope avait rendu possible l'utilisation de signaux visuels pour communiquer sur de grandes distances, mais Hooke avait été incité par un événement à l'origine de bien des avancées technologiques : la guerre. L'année précédente, la ville de Vienne avait failli être capturée par l'armée turque sans que le reste de l'Europe le sache. Soudain, il devint urgent de trouver un moyen d'envoyer des messages rapidement sur de longues distances.

Hooke proposa la construction d'un système de tours disposées dans toute l'Europe. Lorsqu'un message était envoyé du haut de la tour, il était relayé par les tours environnantes — version bidimensionnelle du procédé de diffusion de messages le long de la Grande Muraille de Chine. La méthode de transmission des messages n'était pas très sophistiquée : de grands caractères devaient être hissés dans la mâture à l'aide de cordes. La proposition de Hooke ne fut jamais mise en application, et il fallut attendre une centaine d'années pour qu'une idée similaire voie le jour.

En 1791, les frères Claude et Ignace Chappe conçurent un système de communication pour que le gouvernement révolutionnaire puisse recevoir et envoyer des messages dans les plus brefs délais (un de ces appareils fut attaqué après que la foule l'eut pris pour un moyen de communication entre partisans du roi). Les frères s'inspiraient d'un système qu'ils avaient mis au point quand, internes dans un pensionnat très strict, ils avaient cherché à s'envoyer des messages entre dortoirs. Après de nombreuses expérimentations d'envois de messages par divers procédés visuels, ils adoptèrent finalement un système à base de bras en bois articulés d'une grande lisibilité.

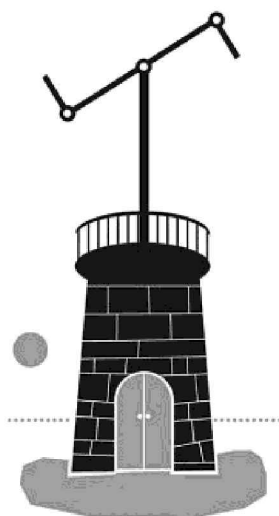


Fig. 4.03 Le code des frères Chappe était transmis par le biais de bras en bois articulés.

Les frères mirent donc au point un code, fondé sur ce système mobile composé d'une traverse et de deux bras en bois, signifiant les différentes lettres de l'alphabet ou divers mots courants. La traverse avait quatre positions, et chacun des deux bras sept positions, ce qui fait un total de $7 \times 7 \times 4 = 196$ positions, ou symboles, différents. Bien qu'une partie du code fût destinée à la communication publique, 92 symboles, combinés en paires, étaient utilisés par les frères comme code secret, ce qui représentait $92 \times 92 = 8\,464$ différents mots ou phrases.

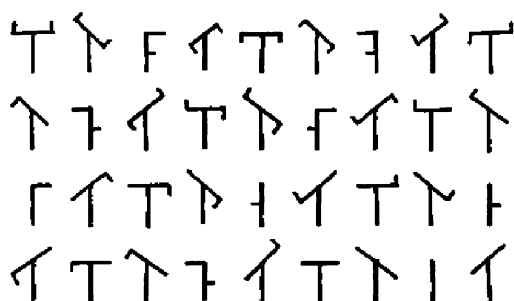


Fig. 4.04 Lettres et chiffres du système de communication inventé par les frères Chappe.

Lors du premier essai du système, le 2 mars 1791, les frères Chappe envoyèrent avec succès le message « Si vous réussissez, vous serez bientôt couvert de gloire » sur une distance de 14 kilomètres. Le gouvernement fut si impressionné par la proposition des deux frères qu'en seulement quatre ans, un réseau de tours et de mâts fut construit à travers toute la France. En 1794, la ligne reliant Paris à Lille, et couvrant une distance de 230 kilomètres, parvint à communiquer avec succès une dépêche annonçant la prise de Condé-sur-L'Escaut, et ce, moins d'une heure après que l'événement eut lieu. Malheureusement, le succès n'amena pas la gloire que semblait promettre le tout premier message. Accusé d'avoir plagié des systèmes de télégraphes existants, Claude Chappe mit fin à ses jours en se noyant dans un puits.

Pour communiquer en mer, les marins ont très tôt utilisé des drapeaux car il suffisait de les brandir depuis une position visible des autres navires. Le message codé sans doute le plus célèbre à être envoyé d'un bateau à un autre à l'aide de drapeaux figure ci-dessous (figure 4.05). Il fut envoyé à 11 h 45 le 21 octobre 1805.

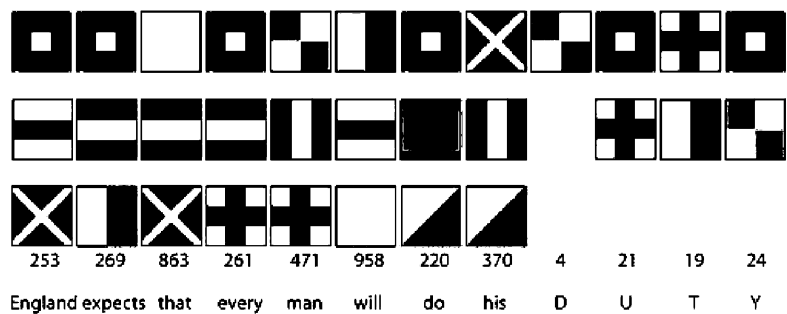


Fig. 4.05 Le célèbre message de l'amiral Nelson. « L'Angleterre attend que chaque homme fasse son devoir. »

Voici le message qu'Horatio Nelson hissa sur son vaisseau amiral *HMS Victory* juste avant que la marine britannique s'engage dans l'affrontement décisif de la bataille de Trafalgar et remporte la victoire. La marine utilisait un code secret élaboré par un autre amiral, sir Home Popham. Les livres d'instructions remis à chacun des bateaux de la marine étaient ourlés de plomb ; ainsi, si le bateau venait à être capturé, le livre d'instructions jeté par-dessus bord coulerait, empêchant l'ennemi de faire main basse sur les chiffres secrets des Britanniques.

Le code se fondait sur des combinaisons de 10 drapeaux différents, chaque drapeau représentant un chiffre de 0 à 9. Les drapeaux étaient hissés en haut du mât trois par trois, indiquant un nombre allant de 000 à 999. Le destinataire du message regardait alors dans le livre des instructions pour voir quel mot était chiffré par un tel nombre. « England » était ici chiffré par le nombre 253, et le mot « *man* » par 471. Certains mots comme « *duty* » ne figuraient pas dans le livre et nécessitaient qu'on les épelle grâce à des drapeaux réservés aux lettres individuelles. À l'origine, Nelson voulait envoyer le message « *England confides that every man will do his duty* », signifiant qu'il estimait que l'Angleterre *avait confiance* en chaque homme pour faire son devoir, mais l'officier chargé d'envoyer le signal, le lieutenant John Pasco, ne trouvait pas le mot « *confides* » dans le livret. Plutôt que d'épeler ce mot à l'aide de drapeaux individuels, il suggéra poliment à Nelson que « *expects* », présent dans le livret, était un meilleur mot.

Les télécommunications remplacèrent l'usage de drapeaux, mais les marins d'aujourd'hui continuent d'apprendre un système moderne fondé sur l'alphabet sémaphore, consistant à communiquer à l'aide d'un pavillon tenu dans chaque main. Il y a huit positions pour chaque bras, ce qui fait $8 \times 8 = 64$ symboles différents possibles.

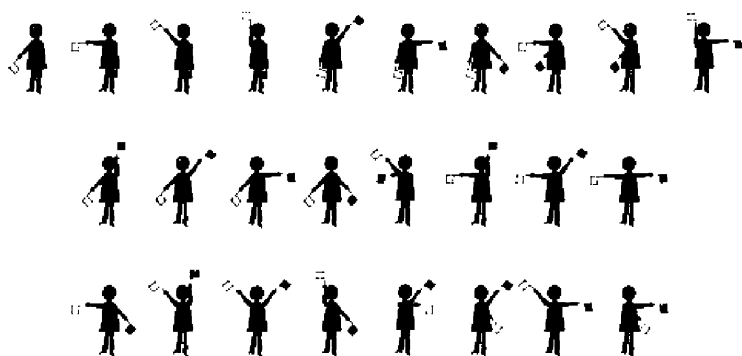


Fig. 4.06 L'alphabet sémaphore.

NUJV !



Fig. 4.07

Sur la pochette de l'album *HELP !*, les Beatles utilisent apparemment les signaux à bras pour annoncer le titre. Mais bien qu'ils utilisent l'alphabet sémaphore, lorsqu'on décode le message il ne dit pas HELP mais NUJV. Robert Freeman, qui eut l'idée d'utiliser le sémaphore pour le concept de couverture, expliqua qu'au « moment de faire la prise de vue, la disposition des bras avec ces lettres n'était pas satisfaisante. Alors on a décidé d'improviser et on a fini avec le meilleur positionnement des bras d'un point de vue graphique ». Voici le geste qu'ils auraient dû faire :



Fig. 4.08

Les Beatles ne sont pas le seul groupe à avoir utilisé un code de manière erronée sur une pochette de disque, ainsi que nous le verrons.

Pour voir comment un message se traduit en sémaphore, allez sur <http://bit.ly/Scoutsemaphore>



Fig. 4.09 Saviez-vous que ce symbole de la paix est un sémaphore ?
À l'origine symbole de la campagne pour le désarmement nucléaire, il représente la superposition des lettres D et N.

QUEL EST LE MESSAGE CODÉ
DE LA CINQUIÈME SYMPHONIE DE BEETHOVEN ?

La *Cinquième Symphonie* de Beethoven débute par une des plus célèbres ouvertures de l’histoire de la musique — trois notes courtes suivies d’une longue. Mais pourquoi, pendant la Seconde Guerre mondiale, la BBC a-t-elle choisi de démarrer tous ses programmes radiodiffusés d’information avec le fameux motif de Beethoven ? Parce que ces quatre notes composent en réalité un message codé. Ce nouveau code était transmis par une série d’impulsions électriques à travers un câble télégraphique.

Une des premières personnes à expérimenter cette forme de communication fut Carl Friedrich Gauss, dont nous avons vu les travaux sur les nombres premiers dans le chapitre 1. Gauss s’intéressait non seulement aux mathématiques mais aussi à la physique, et notamment au nouveau champ d’investigation qu’était l’électromagnétisme. En collaboration avec le physicien Wilhelm Weber, il fit courir un câble d’un kilomètre de long depuis le laboratoire de Weber à Göttingen jusqu’à l’observatoire où il habitait, et ils s’en servirent pour s’envoyer des messages.

Pour ce faire, ils durent concevoir un code. À chaque extrémité du câble, ils installèrent une aiguille rattachée à un aimant entouré de ce même câble. En modifiant le sens du courant, l’aimant tournait vers la gauche ou vers la droite. Gauss et Weber conçurent un code qui traduisait les lettres de l’alphabet et les chiffres de 0 à 9 en combinaisons de rotation vers la droite ou vers la gauche (table 4.04).

d = a	ddd = c,k	gdg = m	gddd = w	ggdd = 4
g = e	ddg = d	dgg = n	ddgg = z	gggd = 5
dd = i	dgd = f,v	dddd = p	dgdg = o	ggdg = 6
dg = o	gdd = g	dddg = d	dggd = 1	gdgg = 7
gd = u	ggg = h	ddgd = s	gddg = 2	dggg = 8
gg = b	ggd = g	dgdd = t	gdgd = 3	gggg = 9

Table 4.04

Excité par les potentialités qu’offrait cette découverte, Weber déclara de manière prophétique :

Lorsque le globe sera recouvert d’un réseau ferroviaire et de câbles télégraphiques, ce réseau offrira des services comparables à ceux du système nerveux dans le corps humain, en partie en tant que moyen de transport, en partie en tant que moyen pour la propagation des idées et des sensations, et ce, à la vitesse de la lumière.

De nombreux codes furent proposés en réponse à cette découverte, mais le code développé par l’Américain Samuel Morse, en 1838, fut une telle réussite qu’il sonna le glas de tous les autres codes. Son code était fondé sur un principe semblable à celui de Gauss et Weber puisque chaque lettre était traduite en une combinaison d’impulsions longues et courtes : des traits et des points.

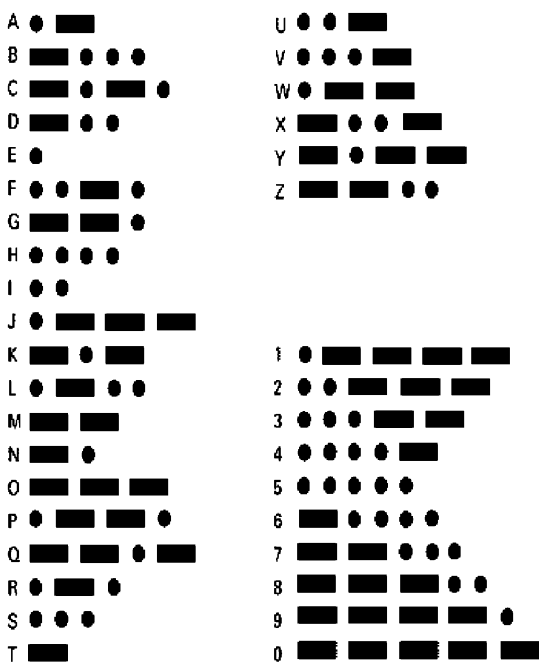


Fig. 4.10 Code Morse.

La logique du code Morse est assez semblable à celle de l’analyse fréquentielle utilisée pour révéler un chiffre de substitution. Les lettres les plus courantes sont le « e » et le « t », donc la logique veut que l’on utilise la plus courte séquence

possible pour les coder. Ainsi, le « e » est représenté par un point, une impulsion courte, et le « t » par un trait, une impulsion longue. Les lettres les moins usitées sont traduites par des séquences plus longues, ainsi « z » devient trait-trait-point-point (ou taah-taah-ti-ti).

Grâce au morse, nous pouvons désormais décoder le message caché dans la *Cinquième Symphonie* de Beethoven. Nous entendons point-point-point-trait (ti-ti-ti-taah), ce qui, en morse, est la lettre « v », que la BBC utilisa donc pour symboliser la victoire.

Bien que Beethoven n'ait jamais eu l'intention de cacher des messages en morse dans sa musique, étant mort bien avant l'invention de ce code, d'autres compositeurs ont, quant à eux, délibérément utilisé des rythmes en morse pour ajouter une strate supplémentaire de sens à leur œuvre. La musique de la série télévisée *Inspecteur Morse* commence de manière pour le moins pertinente par un rythme qui épelle en morse le nom du détective :



Fig. 4.11 « Morse » en code Morse.

Dans certains épisodes, le compositeur a même placé ici et là dans la musique de fond le nom en morse de l'assassin, même s'il s'est également parfois amusé à donner le nom d'un innocent pour tromper les spectateurs capables de déchiffrer le morse.

Très largement utilisé non seulement par les compositeurs mais surtout par les opérateurs de télégraphe dans le monde entier, le morse présente cependant un problème intrinsèque. Si vous recevez un point suivi d'un trait, comment le décoder ? C'est le morse pour la lettre « a » — mais c'est aussi le morse pour la lettre « e » suivie de la lettre « t ». Bref, les mathématiciens ont estimé qu'un autre type de code, à base de 0 et de 1, était bien mieux adapté à l'interprétation par les machines.

QUEL EST LE TITRE DU TROISIÈME ALBUM
DE COLDPLAY ?

Lorsque les fans de Coldplay se précipitèrent en 2005 pour acheter le troisième album du groupe, beaucoup s'interrogèrent sur la signification du concept graphique de la pochette, une série de blocs colorés agencés pour former une grille. Que signifiait cette image ? Il s'agit en réalité du titre de l'album écrit dans un des tout premiers codes binaires, un code conçu en l'occurrence en 1870 par l'ingénieur français Émile Baudot. Les couleurs n'ont aucune espèce d'importance, en revanche chaque bloc représente un 1 et chaque espace un 0.

Le mathématicien allemand Gottfried Leibniz fut au XVII^e siècle l'un des premiers à réaliser l'immense potentiel des 0 et des 1 en tant que moyen efficace de codage de l'information. L'idée lui fut inspirée par l'ouvrage chinois *Yi Jing* — *Le Livre des changements*, qui explore l'équilibre dynamique des contraires. Cet ouvrage présente une série de 64 compositions constituées de traits, appelées des hexagrammes, qui sont censées représenter différents états ou processus. En découvrant ces hexagrammes, Leibniz eut l'idée de créer les mathématiques du binaire (que nous avons abordées dans le chapitre précédent à propos du jeu de Nim). Les symboles se composent d'un empilement de six traits horizontaux, qui peuvent être soit pleins soit interrompus. Le *Yi Jing* explique comment utiliser ces symboles à des fins divinatoires en lançant des bâtons ou des pièces d'argent pour déterminer la structure de l'hexagramme.

Par exemple, si le diseur de bonne aventure obtenait l'hexagramme illustré dans la figure 4.12, cela indiquait le « conflit ». Mais si on remplaçait un trait plein par un trait interrompu, et inversement, on obtenait la figure 4.13, signifiant alors l'« intelligence cachée ».

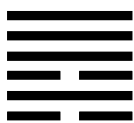


Fig. 4.12

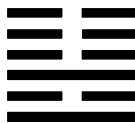


Fig. 4.13

Leibniz s'intéressait surtout au fait que Shao Yong, un savant chinois du XI^e siècle, avait noté que chaque symbole pouvait être associé à un nombre. Si un trait interrompu peut être remplacé par 0 et un trait plein par 1, alors le premier hexagramme peut être lu,

de haut en bas, comme 111010. Dans le système décimal, chaque position correspond à une puissance de 10, et le chiffre qui se trouve à cette position indique combien il faut prendre de puissances de 10. Ainsi, 234 se décompose en 4 unités, 3 dizaines et 2 centaines.

Or Leibniz et Shao Yong ne travaillaient pas en décimal mais en binaire, où chaque position est une puissance de 2. En binaire, le nombre 111010 signifie : aucune unité, un paquet de 2, aucun 4, un paquet de 8, un paquet de 16 et un paquet de 32. Additionnez ces nombres et vous obtenez $2 + 8 + 16 + 32 = 58$. C'est là toute la beauté du binaire : vous n'avez besoin que de deux symboles — au lieu des dix du système décimal — pour représenter n'importe quel nombre. Deux paquets de 16 (décimal) deviennent un paquet de la prochaine puissance de 2, c'est-à-dire 32.

Leibniz comprit que cette manière de représenter les nombres pouvait être d'une redoutable efficacité dès lors qu'il s'agissait de mécaniser les calculs. Les règles concernant l'addition de nombres binaires sont très simples. Pour chaque position, $0 + 1 = 1$, $1 + 0 = 1$ et $0 + 0 = 0$. La quatrième possibilité est $1 + 1 = 0$, qui provoque une retenue, laquelle est reportée et ajoutée à la position suivante sur la gauche. Lorsque nous ajoutons 1000 à 111010, par exemple, nous obtenons un effet domino tandis que les 1 remontent en cascade le nombre :

$$\begin{aligned} 1000 + 111010 &= 10000 + 110010 = 100000 + 100010 = \\ &1000000 + 000010 = 1000010 \end{aligned}$$

Leibniz conçut de magnifiques machines à calculer. L'une d'entre elles consistait en une sorte de boîte munie de trous et équipée d'une petite roue à deux dents qui laissait passer une bille pour représenter les 1 et empêchait la bille de passer pour représenter les 0. Le processus de l'addition devenait alors un fabuleux jeu de flipper mécanique. Leibniz pensait qu'« il est indigne d'hommes remarquables de perdre des heures à un travail d'esclave, le calcul, qui pourrait fort bien être confié à n'importe qui, avec l'aide de machines ». Je pense que la plupart des mathématiciens seraient d'accord.

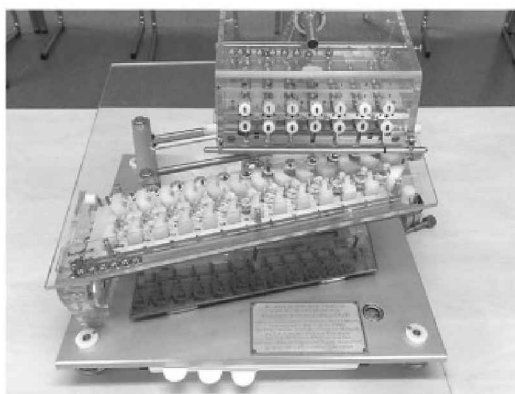


Fig. 4.14 Une reconstitution de la machine arithmétique binaire de Leibniz.

On commença à exprimer, outre les nombres, les lettres de l'alphabet sous la forme d'une série de 0 et de 1. Bien que le morse s'avérât un outil de communication extrêmement efficace entre humains, les machines éprouvaient des difficultés à saisir la différence subtile entre un trait et un point, et pour déterminer avec exactitude quand se terminait une lettre et commençait la suivante.

En 1874, Émile Baudot proposa de coder chaque lettre de l'alphabet par une série de cinq 0 et 1. Chaque lettre ayant la même longueur, son début et sa fin devenaient clairs. L'utilisation de cinq 0 et 1 permit à Baudot de représenter un total de $2 \times 2 \times 2 \times 2 \times 2 = 32$ caractères individuels. La lettre « X » devint ainsi la suite 10111, par exemple, tandis que le « Y » était 10101. Ce fut là une avancée majeure car les messages pouvaient désormais être codés sur des bandes de papier perforées de trous : un trou représentait un 1, et l'absence de trou, un 0. Une machine lisait cette bande puis envoyait le signal via un câble à grande vitesse à un téléscripteur, situé à l'autre bout, qui tapait le message automatiquement.

Au code Baudot succédèrent une pléiade d'autres codes fondés sur cette même idée d'utiliser des 0 et des 1 pour représenter une multitude de choses, qu'il s'agisse de textes, d'ondes sonores, de JPEG ou de fichiers vidéo. Chaque fois que vous allez sur iTunes et que vous téléchargez une chanson de Coldplay, votre ordinateur reçoit une armada de 0 et de 1 que votre lecteur MP3 sait décoder. Dans ces nombres sont contenus les messages qui disent à vos enceintes ou à votre casque audio comment vibrer pour que vous puissiez entendre les tons suaves de Chris Martin. Le fait qu'en

cette époque numérique la musique soit un simple flot de 0 et de 1 est peut-être ce qui inspira le graphiste au moment de créer la pochette du troisième album de Coldplay.

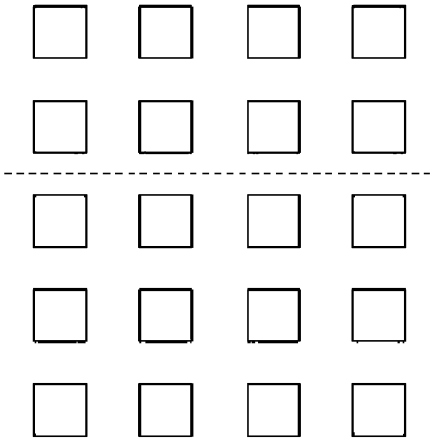


Fig. 4.15 La pochette du troisième album de Coldplay est en code Baudot.

Le code original de Baudot est la clé pour décrypter le message secret contenu dans le graphisme de cette pochette de disque. Le motif peut être divisé en quatre colonnes de cinq blocs. Les blocs de couleur doivent être interprétés comme des 1, et les intervalles comme des 0. Puisqu’il est parfois difficile de distinguer le haut du bas d’une bande, la machine perfore une fine ligne de séparation entre les deux blocs du haut et les trois en dessous. C’est pourquoi il y a un trait qui sépare les blocs gris des blocs de couleur sur la pochette.

La première colonne peut se lire ainsi : couleur-vider-couleur-couleur-couleur, ce qui donne 10111, le code Baudot pour « X ». La dernière colonne représente le code Baudot pour « Y ». Les deux colonnes au centre sont un peu plus intéressantes. Cinq 0 et 1 vous donnent la possibilité de 32 symboles, mais bien souvent nous avons besoin de plus, car il y a aussi les chiffres, les signes de ponctuation et d’autres symboles que nous souhaitons exprimer. Pour faire face à ces exigences, Baudot eut l’idée d’élargir l’éventail des possibles. Tout comme sur un clavier la touche shift, ou maj., permet d’accéder à d’autres symboles à partir des touches usuelles, Baudot utilisa une des séries de cinq 0 et 1 comme un équivalent de

la touche maj. Ainsi, si vous voyez 11011, sachez que la suite suivante appartient à cet éventail de caractères étendus.

Sur ce site Web, vous pouvez créer votre propre pochette d'album Coldplay : <http://bit.ly/Coldcode>

La seconde colonne sur la pochette est précisément la touche maj. de Baudot. Afin de décoder le vide-vide-vide-couleur-couleur de la troisième colonne, nous devons consulter le jeu de caractères étendus détaillé dans le tableau ci-dessous (figure 4.16). Je suis certain que la plupart des gens s'attendent à trouver le symbole pour « & ». Seulement 00011 ne donne pas « & » mais le chiffre 9. Ainsi, le véritable titre du troisième album de Coldplay codé en Baudot est X9Y, et non X&Y. S'agit-il d'une farce de la part de Coldplay ? Probablement pas. Un trou seulement permet de distinguer le « 9 » du « & » dans le code Baudot, il s'agit donc sans doute d'une erreur. Mais cela illustre parfaitement un des problèmes que posent la plupart de ces codes : il est difficile de savoir quand on s'est trompé. C'est dans l'art de détecter une erreur telle que celle-ci que les mathématiques des codes montrent réellement de quoi elles sont capables.

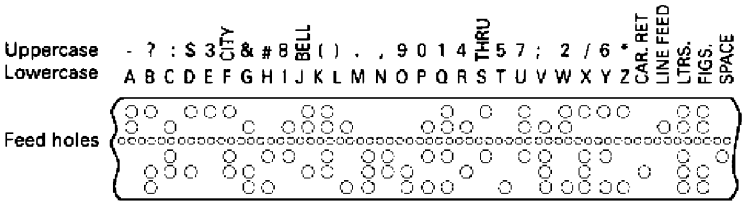


Fig. 4.16 Le code Baudot.

LEQUEL DE CES NOMBRES EST LE CODE D'UN
LIVRE :
0521447712 OU 0521095788 ?

Vous avez certainement déjà remarqué, au dos d'un livre, la présence d'un ISBN (International Standard Book Number). Avec

ses 10 chiffres, l'ISBN identifie un ouvrage donné et nous informe sur son pays d'origine et son éditeur. Mais ce n'est pas tout, car l'ISBN contient aussi une petite part de magie.

Imaginons que je souhaite commander un livre et que je connaisse son ISBN. Je tape le numéro mais, comme je suis pressé, je fais une erreur de saisie. Vous pensez peut-être que je vais du coup recevoir le mauvais livre, mais non, car les ISBN ont une propriété étonnante : ils sont capables d'autodétecter une erreur. Je vais vous montrer comment.

Voici plusieurs authentiques ISBN appartenant à certains de mes livres préférés :

Chiffre de l'ISBN	0	5	2	1	4	2	7	0	6	1	Total
Lorsque multiplié	0	10	6	4	20	12	49	0	54	10	165

Chiffre de l'ISBN	1	8	6	2	3	0	7	3	6	9	Total
Lorsque multiplié	1	16	18	8	15	0	49	24	54	90	275

Chiffre de l'ISBN	0	4	8	6	2	5	6	6	4	2	Total
Lorsque multiplié	0	8	24	24	10	30	42	48	36	20	242

Table 4.05

Sous chacun des chiffres composant l'ISBN, j'ai multiplié le chiffre en question par sa position dans le code. Ainsi, dans le premier ISBN, 0 est multiplié par 1 (ce qui donne 0), 5 par 2 (= 10), 2 par 3 (= 6), et ainsi de suite. Puis, j'ai additionné l'ensemble des produits et j'ai inscrit le résultat dans la colonne du total. Vous ne remarquez rien en voyant ces totaux ? Voici d'autres nombres obtenus par ce même calcul effectué avec d'autres vrais ISBN : 264, 99, 253.

Vous voyez l'élément récurrent ? Le calcul donne toujours un nombre divisible par 11. Loin d'être une étonnante coïncidence, il s'agit plutôt d'un mécanisme mathématique astucieux. Seuls les neuf premiers chiffres contiennent les informations liées à l'identité de l'ouvrage. Le dixième chiffre est ajouté à la série uniquement pour que le nombre total calculé à partir de l'ISBN soit divisible par 11. Il ne vous aura pas échappé que certains livres ont un X au lieu d'un chiffre à la dixième position. Par exemple, l'ISBN

d'un de mes autres livres favoris est 080501246X. Le X est en fait un 10 (pensez aux chiffres romains). Dans ce cas, lorsque vous faites la somme des produits, il vous faut additionner un multiple de 10 en dernière position afin que le total soit divisible par 11.

Si, en saisissant mon ISBN, je me trompe et tape un mauvais chiffre, le calcul me donnera un nombre non divisible par 11 ; l'ordinateur saura alors que je me suis trompé et me demandera de saisir à nouveau l'ISBN. Même si j'inverse deux chiffres, ce qui est courant quand on tape un numéro, l'ordinateur remarquera également l'erreur et, plutôt que de m'envoyer un livre que je n'ai jamais souhaité recevoir, ce sera à moi de renvoyer le bon ISBN. Plutôt malin. Maintenant, à vous de vérifier dans l'intitulé de cette partie quel numéro correspond effectivement à l'ISBN d'un livre et lequel est un imposteur.

Face au nombre sans cesse croissant de livres publiés chaque année, le monde de l'édition n'allait pas tarder à se trouver à court d'ISBN. C'est pourquoi, le 1^{er} janvier 2007, il fut décidé que les ISBN auraient à présent 13 chiffres. 12 chiffres qui identifient le livre, l'éditeur et le pays de publication, et le 13^e pour déceler une possible erreur. Désormais, c'est la divisibilité par 10 et non plus par 11 qui est la clé pour les ISBN à 13 chiffres utilisés par les éditeurs. Jetez un coup d'œil à l'ISBN sur la quatrième de couverture de ce livre. Il a 13 chiffres. Additionnez les 2^e, 4^e, 6^e, 8^e, 10^e et 12^e chiffres et multipliez la somme par 3. Maintenant, ajoutez les autres chiffres. Le total sera divisible par 10. Si vous vous trompez en notant l'ISBN, la plupart du temps, le calcul vous donnera un nombre non divisible par 10.

COMMENT UTILISER LES CODES POUR LIRE DANS LES PENSÉES

Vous aurez besoin de 36 pièces de monnaie pour effectuer ce tour. Donnez à un ami qui ne soupçonne rien 25 pièces et demandez-lui de les disposer de manière à former une grille de 5 × 5, pile ou face, peu importe. Votre ami placera les pièces peut-être ainsi :

F	F	P	P	P
P	P	F	P	P
F	F	F	P	F
P	F	F	P	P
P	P	P	P	P

Table 4.06

Maintenant vous dites : « Dans une minute je vais te demander de retourner une de ces pièces, pile ou face. Puis je lirai dans tes pensées et te dirai quelle pièce tu as retournée. Mais je peux sans doute me rappeler l'ordre de toutes les pièces, alors faisons en sorte que cela soit plus difficile et agrandissons encore le carré. »

Ensuite, vous ajoutez des pièces, apparemment de façon aléatoire, de manière à créer une rangée et une colonne supplémentaires et d'augmenter la grille à $6 \times 6 = 36$... sauf que vous ne disposerez pas du tout des pièces au hasard. Au lieu de cela, vous comptez combien de piles il y a dans chaque rangée et chaque colonne, en commençant par la première colonne. Si le nombre de piles dans cette première colonne est impair, alors la pièce que vous placez en fin de colonne sera côté pile dessus. Si le nombre de piles est pair (0 est considéré comme pair pour notre propos), alors la pièce sera placée côté face dessus.

Répétez l'exercice pour chaque colonne, puis ajoutez une pièce à la fin de chaque rangée selon le même critère. Il ne manque qu'une case vide à remplir dans le coin inférieur droit pour compléter le carré. Choisissez de mettre la pièce côté face ou côté pile visible selon que la colonne au-dessus a un nombre pair ou impair de piles. Il est intéressant de noter que cela reflétera également la parité (c'est-à-dire le caractère pair ou impair) du nombre de piles dans la rangée du bas aussi. Pouvez-vous prouver que cela est toujours vrai ? L'astuce réside dans le fait que ce nombre indique s'il y a un nombre impair ou pair de piles dans la totalité de la grille 5×5 .

Quoi qu'il en soit, la grille a maintenant cette allure :

F	F	P	P	P	P
P	P	F	P	P	F
F	F	F	P	F	P
P	F	F	P	P	P
P	P	P	P	P	P
P	F	F	P	F	F

Table 4.07

Vous êtes maintenant prêt à faire votre tour de magie. Tournez le dos au jeu, et demandez à votre ami de retourner une pièce. Puis revenez face au jeu et concentrez-vous sur la grille tout en annonçant que vous allez maintenant lire dans les pensées de votre ami afin d'identifier la pièce retournée.

Évidemment, vous n'êtes pas extralucide mais plutôt concentré sur la grille initiale 5×5 : vous comptez les piles et les faces de chaque colonne et de chaque rangée afin de déterminer s'il y a un nombre pair ou impair de piles, et vous comparez aux faces et piles ajoutés par vos soins qui indiquent la parité initiale des piles dans chaque colonne et rangée. Si votre ami a retourné une des pièces dans la grille 5×5 , il y a forcément une rangée et une colonne où les pièces ajoutées n'indiquent plus la bonne parité. Observez où la colonne et la rangée « fautives » se croisent : voilà où se trouve la pièce retournée.

Vous devriez à présent pouvoir identifier quelle pièce a été modifiée dans la grille :

F	F	P	P	P	P
F	P	F	P	P	F
F	F	F	P	F	P
P	F	F	P	P	P
P	P	P	P	P	P
P	F	F	P	F	F

Table 4.08

La première colonne dans la grille 5×5 a un nombre pair de piles, mais la pièce que vous avez ajoutée en bas de cette colonne était un pile, ce qui indique qu'à l'origine il y avait un nombre impair de piles. C'est donc dans cette première colonne qu'une pièce a été retournée par votre ami.

Maintenant les rangées. Quelque chose ne tourne pas rond dans la deuxième rangée : le nombre de piles est impair, alors que votre « chiffre de vérification » indique qu'il devrait y avoir un nombre pair de piles. Désormais, tout en faisant comme si vous lisiez dans les pensées de votre ami, vous annoncez : « C'est la pièce se trouvant dans la première colonne, deuxième rangée qui a été retournée. » Applaudissements.

Mais que se passe-t-il si votre ami a retourné une pièce parmi celles que vous aviez rajoutées ? Aucun souci : la pièce dans le coin inférieur droit n'indique plus la parité de la rangée du bas ou de la dernière colonne. Si vous constatez que la pièce n'indique plus la parité de la rangée du bas, vous savez alors qu'une des pièces de cette rangée a été retournée ; vous vérifiez alors chacune des colonnes pour voir laquelle ne correspond plus. Si c'est en fait la sixième et dernière colonne qui ne correspond plus, alors c'est la pièce dans le coin en bas à droite qui a été retournée, et dans ce cas la pièce n'indiquait plus la parité ni de la dernière colonne ni de la rangée d'en bas.

Voici à nouveau la grille, mais avec une de vos pièces retournée. Parvenez-vous à l'identifier ?

F	F	P	P	P	F
P	P	F	P	P	F
F	F	F	P	F	P
P	F	F	P	P	P
P	P	P	P	P	P
P	F	F	P	F	F

Table 4.09

Elle se trouve dans le coin en haut à droite. La pièce côté face dans le coin en bas à droite vous indique qu'il devrait y avoir un nombre pair de piles au-dessus d'elle dans la dernière colonne — or vous avez un nombre impair de piles. Maintenant vérifiez les rangées. La première rangée ne correspond pas car la pièce côté face en fin de rangée vous dit qu'il devrait y avoir un nombre pair de piles à sa gauche. Or, il y a un nombre impair de piles, ce qui vous indique que la pièce dans le coin supérieur droit a été retournée.

Cet exercice présente les fondements de ce qu'on appelle un code correcteur d'erreurs. On l'utilise en informatique pour corriger des erreurs apparues lors des transmissions. Remplacez les piles et les faces par des 0 et des 1, et la grille se transforme en message numérique. Par exemple, chaque colonne dans la grille 5×5 de notre « tour de magie » peut être vue comme représentant un caractère du code Baudot, et la grille dans sa totalité serait alors un message d'une longueur de cinq caractères. La colonne et la rangée supplémentaires sont ajoutées par l'ordinateur pour détecter une éventuelle erreur.

Donc, si nous voulions envoyer le message codé figurant sur la pochette de disque de Coldplay, nous utiliserions une astuce similaire adaptée à une grille 5×4 afin de détecter la présence d'une erreur et, le cas échéant, la localiser. Voici la pochette du disque telle qu'elle aurait dû être composée. Les blocs de couleur ont été remplacés par des 1, les intervalles, ou vides, par des 0 :

1	1	0	1
0	1	1	0
1	0	0	1
1	1	1	0
1	1	1	1

Table 4.10

Maintenant nous ajoutons une colonne et une rangée supplémentaires de 0 et de 1 afin d'indiquer si chaque colonne ou rangée a un nombre pair ou impair de 1 :

1	1	0	1	1
0	1	1	0	0
1	0	0	1	0
1	1	1	0	1
1	1	1	1	0
0	0	1	1	0

Table 4.11

Imaginons qu'une erreur se soit produite pendant la transmission et qu'un des numéros ait été inversé. Le graphiste aurait reçu le message suivant :

1	1	0	1	1
0	1	0	0	0
1	0	0	1	0
1	1	1	0	1
1	1	1	1	0
0	0	1	1	0

Table 4.12

Grâce aux chiffres de vérification dans la dernière colonne et la rangée du bas, le graphiste peut déceler l'erreur. La deuxième rangée et la troisième colonne ne donnent pas un résultat correct. L'erreur se trouve à l'intersection des deux.

Des codes correcteurs comme celui-là sont utilisés pour toutes sortes de choses, des CD aux communications satellitaires. Vous connaissez bien les conversations téléphoniques où l'on n'entend qu'un mot sur deux. Lorsque les ordinateurs se parlent entre eux, ils rencontrent parfois le même problème, mais grâce à l'application de principes mathématiques astucieux nous avons réussi à trouver le moyen de coder des données de manière à nous débarrasser de ces interférences. C'est ce que qu'a fait la NASA lorsque Voyager 2 transmet ses premières images de Saturne. Grâce à l'utilisation d'un code correcteur, les images floues sont devenues d'une netteté étonnante.

COMMENT JOUER SANS TRICHER À PILE OU FACE SUR INTERNET

Les codes correcteurs d'erreurs contribuent à une bonne communication de l'information. Mais nous voulons souvent utiliser notre ordinateur pour envoyer des informations secrètes. Autrefois, que ce soit Marie Stuart reine d'Écosse, lord Nelson ou toute autre personne désireuse d'échanger des messages secrets, il fallait se rencontrer au préalable pour s'accorder sur le code que les deux partis utiliseraient. Aujourd'hui, à l'ère du tout informatique,

nous avons très souvent besoin de transmettre des informations d'ordre privé. Lorsque nous achetons des articles en ligne, nous envoyons notre numéro de carte de crédit à des sites Web. Le commerce sur Internet serait impossible si nous devions encore utiliser l'ancienne cryptographie, qui impliquait de se rencontrer en chair et en os. Heureusement, les mathématiques offrent une solution.

Pour expliquer cette idée, commençons avec un scénario simple. Je veux jouer aux échecs avec quelqu'un sur Internet. J'habite à Londres et mon adversaire à Tokyo. Nous souhaitons déterminer à pile ou face lequel de nous deux jouera en premier. « Pile ou face ? » dit mon e-mail à mon adversaire. Il me répond : « Face. » Je lance la pièce. Je lui renvoie un e-mail qui dit : « Pile, je commence. » Comment peut-il savoir que je n'ai pas triché ?

Étonnamment, il est possible de jouer à pile ou face sur Internet en étant sûr qu'il n'y a pas eu de triche, grâce aux mathématiques des nombres premiers. Tous les nombres premiers sont impairs, sauf le 2. Si nous divisons un de ces nombres premiers impairs par 4, cela nous donne pour reste 1 ou 3. Par exemple, 17 divisé par 4 donne pour reste 1, et 23 divisé par 4, un reste 3.

Comme nous l'avons vu dans le premier chapitre, Euclide a prouvé, il y a deux mille ans, qu'il y a une infinité de nombres premiers. Y en a-t-il une infinité qui ont pour reste 1 (ou 3) dans la division par 4 ? Pierre de Fermat mit les mathématiciens au défi de résoudre ce problème il y a 350 ans, et il fallut attendre le XIX^e siècle pour qu'une réponse soit apportée par le mathématicien allemand Gustav Lejeune Dirichlet. Il présenta des calculs mathématiques extraordinairement compliqués pour montrer que la moitié des nombres premiers donne un reste 1 et l'autre moitié un reste 3 — ni l'un ni l'autre ne sont privilégiés. Le sens exact de « moitié » dans la bouche d'un mathématicien lorsqu'il s'agit de l'infini est compliqué. Mais, essentiellement, cela veut dire que lorsqu'on regarde les nombres premiers inférieurs à n'importe quel nombre en particulier, alors à peu près la moitié d'entre eux auront un reste 1 après division par 4.

Par conséquent, la question du reste 1 ou 3 après division par 4 est aussi hasardeuse que celle de pile ou face. Dans notre problème de lancer de pièce, associons face aux nombres premiers avec un reste 1 après division par 4, et pile aux nombres premiers donnant un reste 3 après la même division. Maintenant, voici l'astuce mathématique. Si je prends deux nombres premiers, disons 17 et 41, tous les deux du tas des faces — ceux qui ont un reste 1 après

division par 4 — et que je les multiplie, la réponse a aussi un reste 1 lorsque divisée par 4. Par exemple, $41 \times 17 = 697 = 174 \times 4 + 1$. Si je prends deux nombres premiers, cette fois du tas des piles, disons le 23 et le 43 — ceux qui ont un reste 3 après division par 4 — ... eh bien, ce n'est pas ce à quoi vous vous attendez. Lorsque je les multiplie, ils donnent aussi un nombre qui a un reste de 1 après division par 4, c'est-à-dire dans notre cas : $23 \times 43 = 989 = 247 \times 4 + 1$. Ainsi, le produit des nombres premiers ne me renseigne en rien sur le tas (pile ou face) dont ils proviennent. C'est ce principe que nous pouvons utiliser pour jouer à « pile ou face sur Internet ».

Si je lance une pièce et obtiens face, je choisis deux nombres premiers du tas des faces et je les multiplie. Si j'obtiens pile, je choisis deux nombres premiers du tas des piles et les multiplie. Une fois que j'ai lancé ma pièce et fait mes calculs, j'envoie ma réponse à mon adversaire à Tokyo. Disons que cela fait 6 497. Puisque la réponse aura toujours pour reste 1 après division par 4, il lui est impossible de déterminer si les deux nombres premiers sont issus du tas des faces ou des piles s'il ne les connaît pas. Maintenant, c'est à lui de dire pile ou face.

Pour savoir s'il a gagné, j'ai juste besoin de lui envoyer les deux nombres premiers que j'ai choisis. Dans notre cas, le 89 et le 73, deux nombres premiers provenant du tas des faces. Étant donné qu'il n'y a pas d'autres nombres premiers dont le produit soit 6 497, je viens de lui donner assez d'informations, en lui communiquant ce nombre 6 497, pour prouver que je n'ai pas triché sans pour autant lui en donner assez pour qu'il puisse, lui, tricher.

En fait, ce n'est pas tout à fait vrai. S'il arrive à déterminer que 6 497 est le produit de 89×73 , alors il sait que c'est face, mais tant que je choisis des nombres premiers très grands (beaucoup plus grands que des nombres à deux chiffres), alors il est quasiment impossible avec les moyens informatiques actuels d'identifier les facteurs (nombres premiers) du produit. Un principe similaire est utilisé dans les codes qui protègent les numéros de carte de crédit que nous envoyons sur le Web.

UN DÉFI FACILE

J'ai fait pile ou face. J'ai pris deux nombres premiers du tas des piles ou du tas des faces et je les ai multipliés entre eux. Le nombre obtenu est 13 068 221. La pièce a-t-elle atterri côté pile ou face ? Essayez de trouver la réponse sans utiliser un ordinateur. (La réponse est donnée en fin de chapitre.)

Un défi difficile

Et si le nombre est :

5 759 602 149 240 247 876 857 994 004 081 295 363 338
151 725 852 938 901 132 472 828 171 992 873 665 524
051 005 072 817 707 778 665 601 229 693 ?

Cette fois, l'utilisation de l'ordinateur est autorisée.

POURQUOI DÉCOMPOSER UN NOMBRE ÉQUIVAUT À CASSER UN CODE

Bob vit en Angleterre et tient une boutique en ligne de maillots de foot. Alice, qui habite à Sydney, veut acheter un maillot sur ce site mais ne souhaite pas que quelqu'un puisse voir ses données de carte bancaire. Bob publie donc un code spécial à base de chiffres sur son site, disons 126 619. Ce numéro de code est l'équivalent d'une clé qui pourra verrouiller le message d'Alice. Ainsi, lorsque Alice se rend sur le site de Bob, elle prend une copie de la clé de codage qui a été publiée et l'utilise pour sécuriser les informations concernant sa carte bancaire.

Ce qui se passe en réalité, c'est que l'ordinateur d'Alice soumet ce numéro à un calcul mathématique spécial. Le numéro de la carte bancaire est maintenant codé et peut être envoyé publiquement sur Internet vers le site Web de Bob. (Vous pouvez voir le détail de ce calcul dans la partie suivante.)

Mais attendez ! N'y a-t-il pas un problème avec cette manière de faire ? Après tout, si je suis un hacker, qu'est-ce qui m'empêche d'aller sur le site de Bob pour prendre une autre copie de la clé afin de déverrouiller le message ? C'est là une chose étonnante concernant ces codes Internet : il faut une tout autre clé pour

déverrouiller la porte, et cette clé est gardée bien au chaud chez Bob.

Cette clé de décodage se compose de deux éléments, en l'occurrence les deux nombres premiers dont le produit égale 126 619, notre numéro de code. Bob a commencé par choisir deux nombres premiers, 127 et 997, afin de créer sa clé de codage (le produit), et ce sont maintenant ces mêmes deux nombres premiers que Bob utilise pour détricoter le calcul mathématique effectué par l'ordinateur d'Alice pour crypter, en premier lieu, son numéro de carte bancaire. Bob a publié la clé de codage 126 619 sur son site Web mais il garde les deux nombres premiers de décodage, 127 et 997, très secrets.

Si je parviens à trouver les deux nombres premiers dont le produit est 126 619, je peux hacker les numéros de carte envoyés au site Web de Bob. Or, 126 619 est assez petit pour que je puisse le diviser par des nombres successifs jusqu'à trouver les nombres premiers 127 et 997 après un temps raisonnable. Mais vous ne pourriez pas utiliser cette méthode avec de vrais sites Web car leurs clés sont fondées sur des nombres bien plus grands — si grands que trouver une paire de nombres premiers en tâtonnant est quasi impossible.

Les mathématiciens à l'origine de ce code sont si sûrs d'eux que pendant de nombreuses années ils proposaient de donner un prix d'un montant de 200 000 dollars à quiconque trouverait les deux nombres premiers dont le produit serait le nombre suivant composé de 617 chiffres :

25 195 908 475 657 893 494 027 183 240 048 398 571 429 282 126
204 032 027 777 137 836 043 662 020 707 595 556 264 018 525 880
784 406 918 290 641 249 515 082 189 298 559 149 176 184 502 808
489 120 072 844 992 687 392 807 287 776 735 971 418 347 270 261
896 375 014 971 824 691 165 077 613 379 859 095 700 097 330 459
748 808 428 401 797 429 100 642 458 691 817 195 118 746 121 515
172 654 632 282 216 869 987 549 182 422 433 637 259 085 141 865
462 043 576 798 423 387 184 774 447 920 739 934 236 584 823 824
281 198 163 815 010 674 810 451 660 377 306 056 201 619 676 256
133 844 143 603 833 904 414 952 634 432 190 114 657 544 454 178
424 020 924 616 515 723 350 778 707 749 817 125 772 467 962 926
386 356 373 289 912 154 831 438 167 899 885 040 445 364 023 527
381 951 378 636 564 391 212 010 397 122 822 120 720 357

Si vous tentiez de cracker ce nombre à 617 chiffres un nombre premier à la fois, vous devriez manipuler plus de nombres qu'il y a d'atomes dans l'univers avant de trouver les deux facteurs. C'est donc sans surprise que personne n'est jamais venu réclamer la récompense et que, pour finir, l'offre fut retirée en 2007.

En plus d'être virtuellement incassables, ces codes à base de nombres premiers présentent une autre caractéristique originale, laquelle permet de résoudre un problème inhérent à tous les codes antérieurs. Avant que ce code à base de nombres premiers ne soit inventé, les codes conventionnels étaient comme une serrure qu'une même clé pouvait à la fois verrouiller et déverrouiller. Les codes Internet sont désormais comme une nouvelle sorte de serrure : une clé la verrouille mais il faut une autre clé pour la déverrouiller. Cela permet à un site Web de diffuser librement des clés pour verrouiller des messages tout en gardant très secrète l'autre clé qui les déverrouille. Vous vous sentez courageux ? Alors voici le détail fascinant du fonctionnement réel de ce code Internet. Commençons par découvrir un calculateur très curieux.

QU'EST-CE QU'UNE HORLOGE MODULAIRE ?

Les codes les plus à la pointe utilisés sur le Web reposent en fait sur une invention mathématique qui précède de plusieurs siècles l'idée même d'Internet : l'horloge modulaire. Dans la prochaine partie, nous étudierons comment ces horloges sont utilisées dans les codes Internet, mais tout d'abord examinons de plus près le fonctionnement d'une telle calculatrice.

Commençons avec une horloge classique dont le cadran est divisé en 12 heures. L'addition sur une telle horloge nous est parfaitement familière — nous savons que quatre heures après 9 heures, il sera 1 heure du matin ou de l'après-midi. C'est la même chose que d'additionner tous les nombres et de déterminer le reste après division par 12, et cela s'écrit ainsi :

$$4 + 9 = 1 \text{ (modulo 12)}$$

Nous écrivons « modulo 12 » car 12 est le module, le point du « retour à la case départ ». Nous pourrions effectuer des sommes similaires sur des horloges ayant différents nombres d'heures au

lieu de rester cantonnés à 12. Par exemple, sur une horloge dont le cadran comporterait 10 heures :

$$9 + 4 = 3 \text{ (modulo 10)}$$

Comment multiplier des nombres sur une horloge modulaire ? Une multiplication consiste à faire une addition un certain nombre de fois. Par exemple, 4×9 revient à prendre quatre 9 et à les additionner. Donc, sur quelle heure aboutira la petite aiguille sur un cadran ordinaire après qu'on a additionné quatre 9 ? $9 + 9$ est la même chose que 6 heures. Chaque fois que nous ajoutons un autre 9, la petite aiguille revient en arrière de trois heures jusqu'à ce que nous parvenions enfin à 12 heures. Comme 0 est un nombre tellement important en mathématiques, nous appelons cela 0 heure sur une horloge modulaire.

Donc nous obtenons cette réponse qui peut sembler étrange :

$$4 \times 9 = 0 \text{ (modulo 12)}$$

Et si nous voulons élever un nombre à une certaine puissance ? Prenons 9^4 , qui revient à multiplier 9 par lui-même 4 fois. Nous venons d'apprendre comment faire une multiplication modulaire, donc cela ne devrait pas être trop difficile. Comme les nombres deviennent plutôt grands, ce sera plus facile de prendre le reste après division par 12 plutôt que d'essayer de courir après les heures autour du cadran. Commençons avec 9×9 , 81. Quel est le reste après division par 12 — en d'autres termes, qu'est-ce que 81 heures sur l'horloge ? C'est en fait à nouveau 9. Et peu importe le nombre de fois qu'on multiplie 9 avec lui-même, on aboutit toujours à 9 :

$$\begin{aligned} 9 \times 9 &= 9 \times 9 \times 9 = 9 \times 9 \times 9 \times 9 = 9^4 \\ &= 9 \text{ (modulo 12)} \end{aligned}$$

La réponse sur une horloge modulaire est obtenue en calculant la réponse sur une calculatrice normale puis en prenant le reste obtenu après division par le nombre d'heures sur l'horloge. Mais la force de l'horloge modulaire réside dans le fait que, souvent, il n'est pas nécessaire de faire des calculs au préalable sur une calculatrice conventionnelle. Pouvez-vous calculer 7^{99} sur une horloge modulaire de 12 heures ? Astuce : calculez 7×7 d'abord, puis multipliez le reste par 7 à nouveau. Vous voyez la règle apparaître ?

Fermat fit une découverte fondamentale concernant les calculs à l'aide d'une horloge modulaire ayant un nombre premier d'heures, disons p , sur son cadran. Il s'aperçut que lorsqu'on prend un nombre sur cette calculatrice et qu'on l'élève à la puissance p , on obtient toujours le nombre avec lequel on a commencé. Cette découverte s'appelle le petit théorème de Fermat, afin de le distinguer du célèbre « dernier » théorème du mathématicien.

La table 4.13 présente plusieurs calculs effectués sur des horloges modulaires ayant un nombre premier ou non premier d'heures.

Nous savons que 5 est un nombre premier ; si je calcule 2 à la puissance 5 sur une horloge modulaire à 5 heures, la réponse est 2 à nouveau. Donc $2^5 = 2$ (modulo 5). Dès lors que le nombre d'heures sur l'horloge est un nombre premier, ce tour de magie fonctionnera toujours. En revanche, dans le cas contraire, cela ne marche pas forcément. Par exemple, 6 n'est pas un nombre premier, et 2^6 donne non pas 2 mais 4.

Puissance de 2	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
Avec une calculatrice conventionnelle	2	4	8	16	32	64	128	256	512	1024
Avec une horloge modulaire à 5 heures	2	4	3	1	2	4	3	1	2	4
Avec une horloge modulaire à 6 heures	2	4	2	4	2	4	2	4	2	4

Table 4.13

Tandis que la petite aiguille avance et indique les heures, une sorte de schéma apparaît. En effet, après $p - 1$ étapes, on est certain, lors de l'étape suivante, de revenir au point de départ ; donc, le modèle se répète toutes les $p - 1$ étapes. Parfois cela se

répète plusieurs fois pendant les $p - 1$ étapes. Sur une horloge de 13 heures, voici ce qu'on obtient pour les puissances 1 à 13 de 3 (c'est-à-dire $3^1, 3^2$ jusqu'à 3^{13}) :

3, 9, 1, 3, 9, 1, 3, 9, 1, 3, 9, 1, 3

La petite aiguille ne passe pas par toutes les heures sur l'horloge, mais il y a cependant toujours ce motif récurrent qui la ramène sur 3 heures dès lors que 3 a été multiplié 13 fois par lui-même.

Nous avons déjà eu affaire à ce type d'arithmétique dans le chapitre 3, lorsque nous regardions comment tricher au poker grâce au *perfect shuffle*. Nous avons varié le nombre de cartes à jouer d'un paquet et nous étions demandé combien de « brassages parfaits » étaient nécessaires pour que le paquet retrouve son ordre initial. Un paquet contenant $2N$ cartes peut nécessiter jusqu'à $2N - 2$ brassages, mais parfois bien moins. Alors qu'un paquet de 52 cartes n'a besoin que de 8 *perfect shuffles* pour retrouver son ordre initial, un paquet de 54 cartes en exigera 52 !

Fermat ne donna jamais le détail de son raisonnement, et il laissa aux futures générations de mathématiciens le soin d'expliquer sa découverte et de montrer pourquoi cela fonctionne toujours pour les horloges portant un nombre premier d'heures. C'est Leonhard Euler qui releva le défi et apporta la preuve du petit théorème de Fermat.

LE PETIT THÉORÈME DE FERMAT

Voici une explication du petit théorème de Fermat. Le théorème dit que, sur une horloge à p heures, p étant un nombre premier,

$$A^p = A \text{ (modulo } p)$$

La preuve est difficile, mais pas compliquée : il suffit de rester bien concentré.

Commençons avec un cas facile pour nous échauffer. Si $A = 0$, le théorème est vrai car, quel que soit le nombre de fois que nous multiplions 0 par lui-même, nous obtenons toujours 0. Donc, supposons que A est différent de zéro. Nous allons montrer que si nous multiplions A par lui-même $p - 1$ fois sur cette horloge, alors nous arrivons à 1 heure sur le cadran. Ceci suffit à prouver le théorème, car en multipliant par A , $A = A^p$.

Premièrement, nous faisons la liste de toutes les heures sur l'horloge, à l'exception de 0. Il y en a $p - 1$:

$$1, 2, \dots, p - 1$$

Puis, nous multiplions chaque nombre dans la liste par A sur notre horloge modulaire, et obtenons :

$$A \times 1, A \times 2, \dots, A \times (p - 1) \text{ (modulo } p)$$

Laissez-moi vous montrer pourquoi les heures dans cette liste doivent être exactement les mêmes que celles dans la liste initiale, $1, 2, \dots, p - 1$, mais dans un ordre différent. Si tel n'était pas le cas, alors soit une des réponses est 0, soit deux réponses sont identiques. Rien d'autre n'est envisageable, car il n'y a que p heures sur l'horloge.

Supposons que $A \times n$ et $A \times m$ donnent la même heure sur l'horloge à p heures où n et m se situent entre 1 et $p - 1$ (je montrerai pourquoi cela signifie que $n = m$). Donc $A \times n - A \times m = A \times (n - m)$ est zéro sur l'horloge modulaire, c'est-à-dire que $A \times (n - m)$ sur notre calculatrice ordinaire est divisible par p .

La clé de la prochaine étape de la preuve est d'utiliser le fait que p est un nombre premier. À l'instar d'une molécule chimique, le nombre $A \times (n - m)$ est construit en multipliant les atomes nombres premiers qui constituent A par les atomes nombres premiers qui constituent $n - m$. Rappelons-nous que p est un nombre premier — un des atomes de l'arithmétique qui ne peut être divisé davantage. Étant donné que p divise $A \times (n - m)$ sans laisser de reste, il doit être un des atomes utilisés pour construire $A \times (n - m)$ car il n'y a qu'une seule façon de construire un nombre en multipliant des nombres premiers. Mais p ne divise pas A sans laisser de reste, il doit donc faire partie de la liste des atomes utilisés pour construire $n - m$. En d'autres termes, $n - m$ est divisible par p . Mais que cela signifie-t-il au juste ? Cela signifie que n et m sont la même heure sur notre horloge de p heures. Il est possible d'utiliser un argument similaire pour prouver que $A \times n$ ne peut pas être zéro heure si ni A ni n ne sont zéro heure.

Notons qu'il est très important que l'horloge ait un nombre premier d'heures — nous avons vu précédemment que 4×9 est zéro sur l'horloge de 12 heures sans que 4 ou 9 soit zéro.

Désormais, nous avons deux listes, $1, 2, \dots, p - 1$ et $A \times 1, A \times 2, \dots, A \times (p - 1)$, composées des mêmes nombres mais dans un ordre différent. Ici, nous pouvons utiliser une petite ruse, que Fermat lui-même avait probablement découverte. Si nous multiplions entre eux tous les nombres sur l'une ou l'autre liste, nous obtenons le même résultat, car l'ordre des facteurs n'a pas d'importance. La première liste nous donne $1 \times 2 \times \dots \times (p - 1)$, que nous pouvons écrire sous la forme de $(p - 1)!$ La seconde liste consiste en A multiplié par lui-même $p - 1$ de fois, et à nouveau 1 à $p - 1$ multipliés entre eux. Après réorganisation des éléments cela nous donne $(p - 1)! \times A^{p-1}$. Et ceux-ci donnent la même réponse sur notre horloge modulaire :

$$(p - 1)! = (p - 1)! \times A^{p-1} \text{ (modulo } p)$$

Ce qui veut dire que $(p - 1)! \times (1 - A^{p-1})$ est divisible par p , et nous utilisons la même astuce qu'auparavant. Aucun des nombres $1, 2, \dots, p - 1$ n'est divisible par p , donc $(p - 1)!$ ne peut pas être divisible par p . La seule possibilité est que $1 - A^{p-1}$ est divisible par p . Et cela signifie que le calcul A^{p-1} sur l'horloge modulaire donne toujours la réponse 1 ; exactement ce que Fermat avait mis les mathématiciens au défi d'expliquer.

Il y a plusieurs ingrédients intéressants dans cet argument. Il est certes important de savoir que si $A \times B$ est divisible par un nombre premier p , alors A ou B doit également être divisible par ce même nombre premier, phénomène lié aux propriétés très spéciales des nombres premiers. Mais, pour moi, le moment le plus beau est lorsqu'on voit la même chose (cette liste de nombres $1, 2, \dots, p - 1$) de deux manières différentes. La pensée latérale dans toute sa splendeur.

COMMENT ENVOYER DES MESSAGES SECRETS SUR INTERNET AVEC UNE HORLOGE

Nous sommes à présent presque prêts pour comprendre comment ces horloges sont utilisées afin d'envoyer des messages secrets sur le Net.

Lorsque vous achetez quelque chose sur un site Web, votre numéro de carte bancaire est codé par votre ordinateur qui utilise l'horloge publique du site, donc le site a besoin de dire à votre ordinateur combien il y a d'heures sur cette horloge. C'est là le premier des deux numéros que votre ordinateur reçoit. Appelons ce numéro N . Dans notre exemple d'e-boutique de maillots de foot, ce numéro était 126 619. Ensuite, appelons E le second numéro d'encodage dont votre ordinateur aura besoin pour faire le calcul. Votre numéro de carte bancaire C est encodé en l'élevant à la puissance E , suivant le calcul effectué par l'horloge modulaire à N heures. De cette manière vous obtenez le nombre C^E (modulo N) codé, et c'est ce numéro que votre ordinateur envoie au site Web.

Mais comment le site déchiffre-t-il ce numéro ? Tout simplement grâce à la magie des nombres premiers de Fermat. Supposons que N soit un nombre premier. (Nous verrons plus tard que cela n'est pas forcément suffisant pour créer un code sécurisé, mais cela nous aidera à comprendre le cheminement.) Si nous multiplions le nombre C^E par lui-même suffisamment de fois, alors

C réapparaîtra comme par magie. Mais à quelle puissance — appelons-la D — devons-nous élever C^E ? Autrement dit, quand est-ce que $(C^E)^D = C$ sur l'horloge à p heures ?

Bien sûr, si $E \times D = p$, cela fonctionne. Mais p est un nombre premier — c'est donc impossible. Maintenant, si nous continuons de multiplier C par lui-même, alors il y a un autre moment où C réapparaîtra obligatoirement à nouveau en tant que réponse. Le numéro de la carte bancaire n'apparaît que lorsque nous l'élevons à la puissance $2(p - 1) + 1$. Et à nouveau quand nous l'élevons à la puissance $3(p - 1) + 1$. Donc, pour trouver le nombre de déchiffrement, nous devons identifier un D tel que $E \times D = 1$ (modulo $(p - 1)$). Cette équation-là est bien plus facile à résoudre. Cependant, comme E et p sont des nombres publics, il est également facile pour un pirate de trouver le chiffre de décodage D . Pour le sécuriser, nous devons utiliser une découverte faite par Euler portant sur les horloges de $p \times q$ heures, et non pas juste de p heures.

Si l'on choisit une heure C sur une horloge ayant $p \times q$ heures, combien de temps avant que $C, C \times C, C \times C \times C \dots$ se répète ? Euler a découvert que le schéma se répète après $(p - 1) \times (q - 1)$ étapes. Donc, pour revenir à l'heure initiale, il faut élever C à la puissance $(p - 1) \times (q - 1) + 1$, ou $k \times (p - 1) \times (q - 1) + 1$, k étant le nombre de fois nécessaires pour que le schéma se répète.

Ainsi, nous savons désormais que pour décoder un message C^E sur une horloge à $p \times q$ heures, nous devons trouver un nombre décodeur D tel que $E \times D = 1$ (modulo $(p - 1) \times (q - 1)$), donc nous devons faire un calcul sur une horloge modulaire secrète à $(p - 1) \times (q - 1)$ heures. Un pirate ne connaît que les nombres N et E et, s'il veut découvrir l'horloge secrète, il doit trouver les nombres premiers secrets p et q . Casser un code Internet revient donc à casser un nombre N en ses blocs de construction, les nombres premiers. Et comme nous l'avons vu lorsque nous avons joué à pile ou face sur Internet, c'est quasiment impossible avec de grands nombres.

Regardons maintenant le code Internet en action, mais avec de très petits p et q afin de faciliter la compréhension. Admettons que pour sa boutique en ligne, Bob ait choisi les nombres premiers 3 et 11 ; ainsi, l'horloge modulaire publique que les clients doivent utiliser pour crypter leur numéro de carte bancaire comporte 33 heures. Bob garde secrets les nombres premiers 3 et 11 car ils sont la clé pour décoder les messages, même s'il rend public le

nombre 33 car c'est le nombre d'heures sur horloge modulaire publique. La seconde information rendue publique sur le site de Bob est le nombre de codage E — disons que c'est 7. Pour chaque personne qui achète un maillot de foot sur le site de Bob en ligne, il se passe exactement la même chose : leur numéro de carte bancaire est élevé à la puissance 7 sur une horloge modulaire à 33 heures.

Un des clients de la boutique en ligne de Bob a une des toutes premières cartes bancaires qui soient, dont le numéro est 2. En élevant 2 à la puissance 7 sur une horloge modulaire de 33 heures, nous obtenons 29.

Voici une manière astucieuse de calculer 2^7 sur l'horloge modulaire à 33 heures. Commençons par multiplier des 2 ensemble : $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 32$. Tandis que les puissances de 2 augmentent, la petite aiguille poursuit son chemin autour du cadran, et lorsque nous arrivons au stade où nous multiplions par 2 une sixième fois, la petite aiguille fait plus qu'un tour complet. Il y a une petite astuce que nous pouvons appliquer ici qui donne l'impression que l'aiguille va à rebours au lieu d'avancer. Il suffit de dire que 32 heures sur notre horloge modulaire de 33 heures est -1 heure. Puis, après être parvenu à $2^5 = 32$, deux multiplications supplémentaires par 2 nous amèneront à -4 , ou 29 heures. De cette façon, nous évitons de calculer 2 à la puissance 7 (c'est-à-dire 128), puis de trouver le reste après division par 33. Dans le cas de très grands numéros, ce genre de raccourci est extrêmement précieux pour un ordinateur dont l'objectif est de calculer très rapidement.

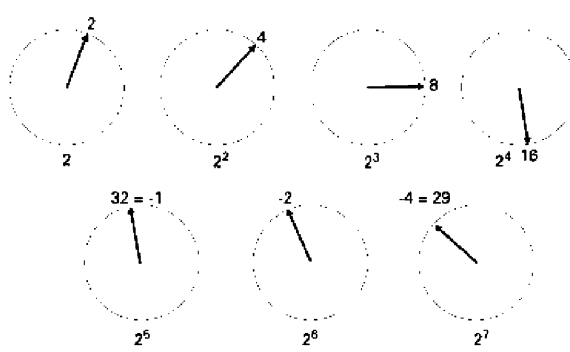


Fig. 4.17 Calculs de puissances sur une horloge modulaire à 33 heures.

Comment être sûr que le numéro chiffré du client, 29, est sécurisé ? Après tout, un hacker peut voir ce numéro se balader dans le cyberspace et peut facilement se renseigner sur la clé publique de Bob, laquelle consiste en une horloge modulaire de 33 heures et l'instruction d'élever le numéro de la carte bancaire à la puissance 7. Pour casser ce code, il suffit au pirate de trouver un nombre qui, multiplié par lui-même 7 fois sur une horloge modulaire de 33 heures, donnera la réponse 29.

Inutile de préciser que ce n'est pas aussi facile que ça. Même avec des calculs arithmétiques normaux, calculer le carré de nombres peut se faire au dos d'une enveloppe, mais c'est bien plus difficile de déconstruire le processus et de chercher la racine carrée. La difficulté supplémentaire vient du calcul des puissances sur une horloge modulaire. Très vite on perd de vue le point de départ tant la taille de la réponse n'a plus aucun rapport avec l'endroit où on a commencé.

Dans notre exemple, les nombres sont assez petits pour qu'un pirate puisse essayer toutes les variantes pour trouver la réponse. Dans la pratique, les sites Web utilisent des horloges dont le nombre d'heures a plus de 100 chiffres, rendant impossible une recherche exhaustive. Vous vous demandez peut-être comment, s'il est déjà aussi difficile de résoudre ce problème sur une horloge modulaire de 33 heures, un site marchand sur Internet est capable de récupérer le numéro de carte bancaire d'un client.

La version plus générale proposée par Euler du petit théorème de Fermat garantit l'existence d'un nombre décodeur magique, D . Bob peut multiplier le numéro de carte bancaire codé par lui-même D fois afin de révéler le numéro original de la carte bancaire. Mais D ne peut être élucidé qu'à condition de connaître les nombres premiers secrets p et q . La connaissance de ces deux nombres premiers est alors la clé pour déverrouiller les secrets de ce code Internet, car il faut résoudre le problème suivant sur l'horloge modulaire secrète :

$$E \times D = 1 \text{ (modulo } (p - 1) \times (q - 1))$$

Lorsque nous remplaçons E , p et q par nos nombres, nous voyons qu'il nous faut résoudre l'équation suivante :

$$7 \times D = 1 \text{ (modulo } (2 \times 10))$$

Ce qui revient à nous demander de trouver un nombre qui, multiplié par 7, donne un nombre avec un reste 1 après division par 20. $D = 3$ fonctionnera car $7 \times 3 = 21 \equiv 1 \pmod{20}$.

Et si nous élevons notre numéro codé de carte bancaire à la puissance 3, le numéro initial de la carte bancaire réapparaît :

$$29^3 \equiv 2 \pmod{33}$$

Ainsi, pour récupérer le numéro de carte bancaire à partir du message codé, il faut connaître les nombres premiers secrets p et q ; par conséquent, quiconque veut hacker les codes sur le Net doit trouver le moyen de prendre un nombre N et d'identifier les deux nombres premiers qui le divisent. Chaque fois que vous achetez un livre en ligne ou que vous téléchargez une chanson, vous recourez à la magie des nombres premiers pour sécuriser votre carte bancaire.

LA QUESTION À UN MILLION DE DOLLARS

Les créateurs de codes s'efforcent d'être toujours en avance sur les casseurs de codes ! Les mathématiciens n'ont de cesse d'inventer des manières de plus en plus astucieuses pour envoyer des messages secrets dans l'hypothèse où le chiffrement à base de nombres premiers deviendrait inopérant. Un nouveau « code cryptographique elliptique » (on utilise souvent l'abréviation anglo-saxonne, ECC) est déjà en service pour protéger les routes aériennes des avions, et le défi d'un million de dollars proposé dans ce chapitre est lié à la compréhension arithmétique des courbes elliptiques qui fondent ces nouveaux codes.

Il existe une multitude de courbes elliptiques, mais toutes ont des équations de type $y^2 = x^3 + ax + b$. Chaque courbe correspond à différentes valeurs de a et b : par exemple, $a = 0$ et $b = -2$ nous donne $y^2 = x^3 - 2$.

Cette équation définit une courbe que je peux tracer sur du papier millimétré, comme ci-contre, en calculant un certain nombre de points (x, y) . J'attribue une valeur à x , puis je calcule l'équation $x^3 - 2$ et je prends sa racine carrée pour obtenir la valeur correspondante de y . Par exemple, si $x = 3$, alors $x^3 - 2 = 27 - 2 = 25$. Pour trouver y , je dois chercher la racine carrée de 25,

puisque $y^2 = x^3 - 2$, donc y est 5 ou -5 (car moins fois moins égale plus, il y a toujours deux racines carrées). La représentation graphique obtenue est symétrique par rapport à l'axe horizontal. Ici, nous avons trouvé les deux points (3, 5) et (3, -5).

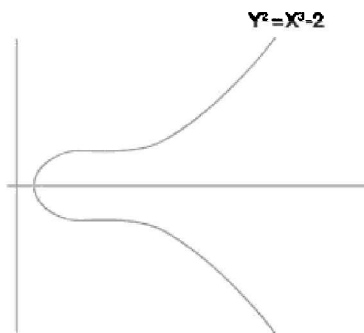


Fig. 4.18 Représentation graphique d'une courbe elliptique.

Ces points sur la courbe elliptique sont bien jolis, car x et y sont des nombres entiers. Pouvez-vous trouver d'autres points tels que ceux-ci ? Essayons avec $x = 2$. Nous avons alors $x^3 - 2 = 8 - 2 = 6$, donc $y = \sqrt{6}$ ou $-\sqrt{6}$. Dans le premier exemple, 25 a pour racine carrée un nombre entier (5), mais la racine carrée de 6 est plus compliquée. Les Grecs anciens apportèrent la preuve qu'il n'existe aucune fraction, et encore moins de nombre entier, qui a pour carré 6. $\sqrt{6}$, écrit sous forme de nombre décimal, se poursuit à l'infini sans aucune répétition d'une série de chiffres (c'est un nombre irrationnel).

$$\sqrt{6} = 2,449489742783178...$$

La question à un million de dollars concerne l'identification des points sur cette courbe où à la fois x et y sont des entiers ou des fractions. La plupart du temps, ce n'est pas le cas, car quand vous placez x , le y ne sera pas un entier ni même une fraction car la plupart des nombres n'ont pas une racine carrée bien nette (c'est-à-dire une racine carrée qui serait un « nombre réel »). Nous avons eu de la chance de trouver que (3, 5) et (3, -5) sont des points sympathiques sur la courbe, mais y en a-t-il d'autres ?

Les Grecs mirent au point un très bel exemple de géométrie par lequel on obtient d'autres points (x , y), où à la fois x et y sont des fractions, dès lors qu'un de ces points a été trouvé. Tracez une ligne qui passe par le premier point trouvé — et soit tangent à la courbe,

comme illustré ci-dessous. Nous appelons cette ligne la tangente à la courbe en ce point. En continuant cette ligne, nous observons qu'elle coupe la courbe en un nouveau point. La beauté de la construction, c'est que les coordonnées de ce nouveau point seront elles aussi toutes deux des fractions.

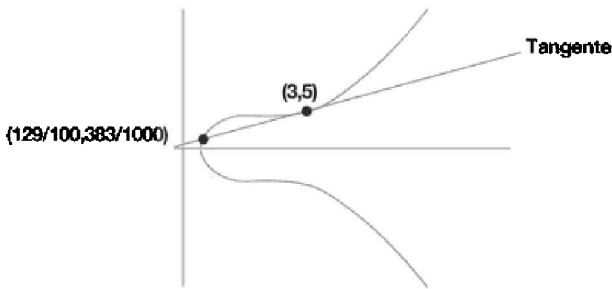


Fig. 4.19 Comment trouver d’autres points sur la courbe elliptique dont les coordonnées sont des fractions.

Par exemple, si nous traçons la tangente au point $(x, y) = (3, 5)$ sur la courbe elliptique $y^2 = x^3 - 2$, nous trouvons qu’elle croise la courbe en un nouveau point, $(x,y) = \left(\frac{129}{100}, \frac{383}{1000}\right)$, où les deux coordonnées sont des fractions. À partir de ce nouveau point, nous pourrions répéter le processus et obtenir un autre point où à la fois x et y sont des fractions :

$$\left(\frac{2\,340\,922\,881}{45\,427\,600}, \frac{93\,955\,726\,337\,279}{306\,182\,024\,000}\right)$$

Sans cette construction géométrique, il serait extrêmement difficile de se rendre compte que pour :

$$x = \frac{2\ 340\ 922\ 881}{45\ 427\ 600}$$

on trouve un y qui est aussi une fraction.

Vous pouvez répéter cette géométrie et obtenir des paires de fractions (x, y) infiniment nombreuses qui sont des points sur cette courbe. Pour une courbe elliptique générale $y^2 = x^3 + ax + b$, si on a un point (x_1, y_1) sur la courbe où, à la fois, x_1 et y_1 sont des fractions, alors placer :

$$x_2 = \frac{(3x_1^2 + a)^2 - 8x_1y_1^2}{4y_1^2}$$

et :

$$y_2 = \frac{x_1^6 + 5ax_1^4 + 20bx_1^3 - 5a^2x_1^2 - 4abx_1 - a^3 - 8b^2}{8y_1^3}$$

donnera un autre point sur la courbe où à la fois x_2 et y_2 sont des fractions.

Pour notre courbe $y^2 = x^3 - 2$, cela donne une infinité de points rationnels, où à la fois x et y sont des fractions, mais il y a des courbes où on n'obtient qu'un nombre fini. Par exemple, prenons la courbe définie par l'équation :

$$y^2 = x^3 - 43x + 166$$

Sur cette courbe, il n'y a en réalité qu'un nombre fini de points rationnels :

$$(x, y) = (0, 0), (3, 8), (3, -8), (-5, 16), (-5, -16), (11, 32), (11, -32)$$

Et même, tous ces points sont entiers. Toute tentative géométrique ou algébrique nous fait retomber sur ces sept points.

La question à un million de dollars, appelée la conjecture de Birch et Swinnerton-Dyer, est la suivante : comment déterminer si une courbe elliptique aura une infinité de points dont les deux coordonnées seront des entiers ou des fractions ?

Vous vous demandez peut-être : qui s'en soucie ? Eh bien, tous autant que nous sommes, car le calcul de courbes elliptiques est aujourd'hui utilisé dans les domaines de la téléphonie mobile et des cartes à puce pour protéger nos données privées, tout comme dans celui du contrôle aérien pour assurer notre sécurité. Grâce à ce nouveau type de code, votre numéro de carte bancaire ou votre message est converti par un calcul astucieux en un point sur cette courbe. Pour chiffrer le message, un autre point à partir d'un point donné est identifié grâce à ce calcul mathématique fondé sur l'utilisation du principe géométrique étudié plus haut qui, nous l'avons vu, génère de nouveaux points.

« Inverser » cette procédure géométrique nécessiterait des calculs mathématiques qu'à l'heure actuelle nous ne savons pas faire. Mais si vous trouvez la solution à ce problème d'un million de dollars, alors cela veut dire que vous êtes également capable de casser ces codes, auquel cas vous n'aurez que faire de ce million de dollars puisque vous serez le plus puissant pirate de la planète.

SOLUTIONS

Chiffre de substitution déchiffré

A mathematician, like a painter or a poet, is a maker of patterns.

(Un mathématicien, comme un peintre ou un poète, est créateur de formes.)

If his patterns are more permanent than theirs, it is because they are made with ideas. The mathematician's patterns, like the painter's or the poet's, must be beautiful; the ideas like the colours or the words, must fit together in a harmonious way. Beauty is the first test: there is no permanent place in the world for ugly mathematics.

(Les formes créées par le mathématicien, comme celles créées par le peintre ou le poète, doivent être belles ; les idées, comme les couleurs ou les mots, doivent s'agencer harmonieusement. La beauté est le premier critère : il n'y a pas en ce monde de place permanente pour des mathématiques laides.)

Le chiffre est :

Texte clair	a	b	c	d	e	f	g	h	i	j	k	l	m
Texte chiffré	B	A	N	T	S	H	U	F	L	K	X	I	O
Texte clair	n	o	p	q	r	s	t	u	v	w	x	y	z
Texte chiffré	C	M	Q	P	V	E	D	G	R	Z	W	J	Y

Table 4.14

Un défi facile

La pièce a atterri côté face dessus. $13\,068\,221 = 3\,613 \times 3\,617$. À la fois 3 613 et 3 617 sont des nombres premiers qui ont un reste 1 après division par 4. Il y a un moyen de factoriser ce nombre rapidement, grâce à la méthode découverte par Fermat. Si vous

élevez au carré 3 615, vous obtenez 13 068 225, qui est à 4 de 13 068 221. 4 est également un carré. Maintenant, avec un peu d'algèbre vous indiquant que $a^2 - b^2 = (a + b) \times (a - b)$, vous obtenez :

$$\begin{aligned} 13\,068\,221 &= 3\,615^2 - 2^2 \\ &= (3\,615 + 2) \times (3\,615 - 2) = 3\,613 \times 3\,617 \end{aligned}$$

Chapitre V

PEUT-ON PRÉDIRE LE FUTUR ?

S'il était possible de voyager dans le temps, prédire l'avenir serait facile : il me suffirait de revenir de l'année prochaine et de vous dire ce qui va se passer. Hélas, nous ne savons pas voyager dans le temps, et les nombreux moyens par lesquels certains prétendent prédire l'avenir — boule de cristal ou horoscope — sont discutables. Si vous voulez vraiment savoir ce qui se passera demain, l'année prochaine ou au prochain millénaire, il vaut mieux s'en remettre à nouveau aux mathématiques.

Les mathématiques peuvent prévoir si la Terre sera heurtée par un astéroïde et pendant combien de temps le Soleil continuera de brûler. Mais il reste certaines choses que même les mathématiciens ont du mal à prévoir. Nous avons les équations qui doivent expliquer, par exemple, la météo, la croissance de la population et la turbulence dans la traînée d'un ballon de football en mouvement, mais nous ne savons pas résoudre la plupart d'entre elles. Le prix d'un million de dollars pour ce chapitre ira à la personne capable de résoudre les équations de la turbulence et de prédire la suite des événements.

La capacité des mathématiques à prédire l'avenir a donné à ceux qui les maîtrisent un grand pouvoir. Depuis les tout premiers astronomes qui pouvaient prédire les mouvements des planètes dans le ciel nocturne, jusqu'aux gestionnaires de fonds spéculatifs qui prévoient aujourd'hui les fluctuations des prix sur le marché boursier, nombreux sont ceux qui ont tiré profit des mathématiques pour plonger dans l'avenir. Et s'il est vrai qu'une partie des mathématiques modernes est diaboliquement difficile, ses praticiens, plutôt que de nous laisser dans le noir, recherchent sans cesse de nouvelles idées pour apporter un éclairage sur les événements futurs.

COMMENT LES MATHS ONT-ELLES SAUVÉ TINTIN ?

Dans la bande dessinée d'Hergé *Le Temple du Soleil*, Tintin est fait prisonnier par une tribu inca après s'être égaré à l'intérieur du temple du Soleil. Les Incas condamnent Tintin et ses amis, le capitaine Haddock et le professeur Tournesol, à être immolés sur le bûcher. Le feu sera déclenché par une loupe qui concentrera les rayons du Soleil sur le tas de bois. Mais Tintin est autorisé à choisir l'heure de leur mort. Pourra-t-il exploiter cette faveur pour se sauver, lui et ses amis ?

Tintin s'aperçoit qu'une éclipse solaire touchera la région quelques jours plus tard. Il choisit donc l'heure en fonction de ce phénomène. (En réalité, quelqu'un d'autre a fait les calculs et Tintin a juste vu la prédiction dans la presse.) Quelques instants avant l'éclipse, Tintin s'exclame : « Tes invocations ne seront pas entendues par le dieu souverain. Et toi, ô puissant Soleil, montre à tous, par un signe tangible, que tu ne désires pas notre mort. » Et exactement comme prévu selon les calculs, le Soleil disparaît et la tribu terrifiée libère Tintin et ses amis.

Les mathématiques permettent de repérer des modèles, et c'est ainsi qu'elles nous donnent le pouvoir d'explorer l'avenir car les premiers astronomes qui scrutaient le ciel nocturne remarquèrent rapidement que les mouvements de la Lune, du Soleil et des planètes se répétaient. De nombreuses cultures utilisent ces rythmes célestes pour enregistrer le passage du temps. Beaucoup de calendriers différents sont possibles parce que le Soleil et la Lune se meuvent dans le ciel à un rythme fou et syncopé ; mais tous ont une chose en commun : c'est le rôle que jouent les mathématiques dans l'interprétation des cycles du Soleil et de la Lune afin de marquer le temps. On constate par exemple le rôle curieux joué par le nombre 19 pour déterminer quand tombent les fêtes mobiles annuelles, comme Pâques.

L'unité de temps de base commune à tous ces calendriers est le jour de 24 heures. Ce n'est pas le temps qu'il faut à la Terre pour faire un tour sur son axe : celui-ci est un peu moindre, 23 heures 56 minutes et 4 secondes. Si nous utilisions cette durée légèrement plus courte comme longueur d'une journée, notre horloge et la Terre en rotation se décaleraient de plus en plus car ces 3 minutes et 56 secondes s'accumuleraient jusqu'à ce que le midi de l'horloge se produise à minuit. Donc, pour garder l'heure, nous définissons

un jour — ou, pour utiliser le bon terme, un jour solaire — comme le temps qu'il faut au Soleil pour revenir à la même position dans le ciel, observé du même point à la surface de la Terre. Après une rotation complète, la Terre se sera déplacée autour de son orbite d'environ $1/365$ d'une révolution ; il faut donc environ $1/365$ d'une rotation, c'est-à-dire un autre $1/365$ d'un jour — soit environ 3 minutes et 56 secondes —, pour que le Soleil revienne au même endroit dans le ciel.

Pour être un peu plus précis, il faut à la Terre 365,2422 de ces jours solaires pour faire une fois le tour du Soleil. Le calendrier grégorien, utilisé dans la plupart des pays, est fondé sur une bonne approximation de ce cycle. 0,2422 est proche de 0,25, soit d'un quart, donc en ajoutant un jour supplémentaire au calendrier tous les quatre ans, le calendrier grégorien maintient plutôt bien l'allure par rapport à la Terre en orbite autour du Soleil. Quelques petits ajustements sont nécessaires car 0,2422 n'est pas égal à 0,25 ; et c'est pourquoi tous les 100 ans nous laissons passer une année bissextile, et tous les 400 ans au lieu de la laisser passer, nous la gardons.

Le calendrier islamique utilise quant à lui le cycle de la Lune. Dans ce cas, l'unité de base est un mois lunaire, et 12 d'entre eux constituent une année lunaire. Un mois lunaire, dont le début est déterminé par l'observation de la nouvelle lune à La Mecque, est d'environ 29,53 jours, ce qui rend l'année lunaire 11 jours plus courte qu'une année solaire. 365 divisé par 11 donne environ 33, il faut donc 33 ans au mois du ramadan pour parcourir son cycle au travers de l'année solaire, et c'est pourquoi le ramadan se décale chaque année et passe d'une saison à l'autre dans le calendrier grégorien.

Les calendriers juif et chinois mêlent Soleil et Lune, en utilisant le cycle de l'orbite de la Terre autour du Soleil et le cycle de l'orbite de la Lune autour de la Terre. Ils ajoutent un mois bissextile environ tous les trois ans, et la clé des calculs est le nombre magique 19. 19 années solaires ($= 19 \times 365,2422$ jours) correspond presque exactement à 235 mois lunaires ($= 235 \times 29,53$ jours). Le calendrier chinois a 7 années bissextiles dans chaque cycle de 19 années afin que les calendriers lunaire et solaire restent synchrones.

Le nombre 19 aurait été important dans les calculs de Tintin, car la séquence des éclipses du Soleil et de la Lune se répète elle aussi après 19 ans. Cette scène du *Temple du Soleil* s'inspire d'un moment célèbre de l'histoire, quand Christophe Colomb profita

d'une éclipse pour sauver son équipage, alors qu'ils étaient bloqués à la Jamaïque en 1503. Les indigènes, d'abord amicaux, étaient devenus hostiles et refusaient de fournir des vivres à Colomb et son équipage. Menacé par la famine, Colomb imagina un plan ingénieux. Il consulta son almanach (ouvrage contenant les prévisions de marées, les cycles lunaires et les positions des étoiles utilisé par les marins pour la navigation) et vit qu'une éclipse lunaire était annoncée pour le 29 février 1504. Colomb convoqua les indigènes trois jours avant l'événement et les menaça : s'ils ne lui fournissaient pas des vivres, il ferait disparaître la Lune.

QUAND AURA LIEU LA PROCHAINE ÉCLIPSE ?

Si vous connaissez l'heure précise d'une éclipse, vous pouvez calculer celle de la suivante grâce à une équation. Les calculs dépendent de deux nombres importants.

Le premier est le mois synodique (S) de 29,5306 jours. C'est le temps moyen qu'il faut à la Lune pour faire le tour de la Terre et revenir à la même position par rapport au Soleil. C'est le temps moyen entre deux nouvelles lunes.

Le second est le mois draconique (D) de 27,2122 jours. L'orbite de la Lune autour de la Terre est légèrement inclinée par rapport à celle de la Terre autour du Soleil. Les deux orbites se croisent en deux endroits, appelés nœuds de l'orbite lunaire, comme montré à la page suivante. Le mois draconique est le temps moyen qu'il faut à la Lune, à partir d'un nœud, pour rejoindre le nœud opposé et revenir au premier.

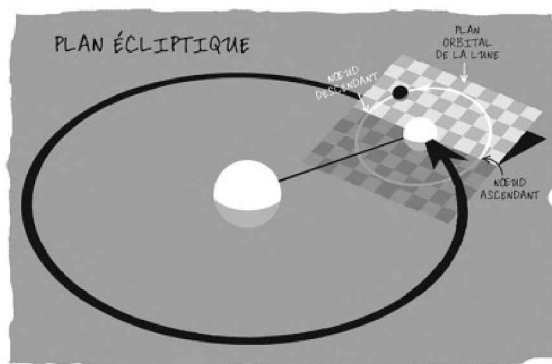


Fig. 5.01 L'orbite de la Lune croise celle de la Terre à deux endroits, appelés nœud ascendant et nœud descendant.

Pour chaque paire de nombres entiers A et B , il est possible de trouver S et D qui rendront $A \times S$ très proche de $B \times D$; vous aurez

alors la date d'une éclipse $A \times S \approx B \times D$ jours après la dernière éclipse observée. Et il y aura une autre éclipse après $A \times S \approx B \times D$ jours. La suite des éclipses continuera pendant un certain temps mais, comme l'équation n'est pas exacte, au bout d'un moment les éclipses seront de moins en moins spectaculaires, jusqu'à ce que le Soleil, la Lune et la Terre ne soient plus alignés. Et ce sera alors la fin de ce cycle particulier d'éclipses.

Voici un exemple :

$A = 223$ mois synodiques est très proche de $B = 242$ mois draconiques ; donc, tous les $223 \times 29,5306 \approx 242 \times 27,2122$ jours après une éclipse, il y en aura une autre, presque identique. Cela fait une période d'environ $6\,585^{1/3}$ jours, ou environ 18 années, 11 jours et 8 heures. Le décalage de 8 heures signifie que les deux prochaines éclipses semblables seront vues d'un endroit différent sur la surface de la Terre. Cependant, la troisième se produira au même endroit ; donc, toutes les trois fois 18 années 11 jours et 8 heures, ou environ 19 756 jours complets, la même éclipse se répète.

Par exemple, l'éclipse lunaire totale visible en Amérique du Nord le 21 décembre 2010 est la répétition de celle du 9 décembre 1992 vue d'Europe. Elle a été vue pour la dernière fois en Amérique le 18 novembre 1956. Il y a eu d'autres éclipses entre ces dates mais elles font partie d'autres cycles d'éclipses qui se déroulent parallèlement à celui-ci. Grâce aux mathématiques, il est possible de calculer la date de la prochaine éclipse au sein de chaque cycle.

Les indigènes, ne croyant pas que Colomb ait le pouvoir de faire disparaître la Lune, n'apportèrent pas de nourriture. Mais le soir du 29 février, quand la Lune apparut à l'horizon, ils purent voir qu'il en manquait déjà un morceau. D'après le fils de Colomb, Ferdinand, quand la Lune finit par s'estomper dans le ciel, les indigènes furent terrifiés et « avec force hurlements et lamentations accoururent de partout vers les bateaux, chargés de vivres, suppliant l'amiral d'intercéder pour eux auprès de son dieu ». Par un calcul précis, Colomb fit coïncider son pardon avec la réapparition progressive de la Lune. Ce récit est peut-être apocryphe, ou enjolivé par les Espagnols pour glorifier l'intelligence des conquérants venus d'Europe face à l'ignorance de ces indigènes. Mais il n'en montre pas moins la puissance des mathématiques.

La capacité des mathématiques à prévoir des événements dans le ciel nocturne repose sur l'observation de phénomènes qui se répètent. Mais comment prévoir le nouveau ? Le récit de notre utilisation d'équations pour explorer l'avenir commence par la

prévision du comportement d'objets simples, comme le ballon de football.

SI JE FAIS TOMBER UNE PLUME ET UN BALLON, LEQUEL ARRIVE AU SOL LE PREMIER ?

Le ballon bien entendu. Pas la peine d'être un mathématicien de renom pour prévoir cela. Et s'il s'agit de deux ballons de football de même diamètre, l'un contenant du plomb et l'autre de l'air ? La plupart des gens répondent intuitivement que le ballon plombé touchera le sol le premier. C'est certainement ce que croyait Aristote, l'un des plus grands penseurs de tous les temps.

Par une expérience apocryphe, le savant italien Galilée a montré que cette réponse intuitive est complètement erronée. Il travaillait à Pise, ville de la célèbre tour penchée. Quel meilleur endroit pour jeter des objets en demandant à son apprenti, posté en bas, de voir lequel arrive le premier. Galilée prouva qu'Aristote avait tort : les deux ballons, quoique de poids différents, touchèrent le sol en même temps.

Galilée comprit que le poids de l'objet ne jouait aucun rôle. Si une plume tombe plus lentement qu'un ballon, c'est à cause de la résistance de l'air. Si l'on pouvait éliminer l'air, les deux tomberaient à la même vitesse. Cette théorie pourrait être testée sur la Lune où il n'y a pas d'atmosphère. En 1971, le commandant de la mission Apollo 15 sur la Lune, David Scott, reproduisit l'expérience de Galilée en laissant tomber en même temps un marteau de géologue et une plume de faucon. Leur chute fut beaucoup plus lente que sur la Terre, en raison de la force de gravité inférieure sur la Lune, mais les deux objets touchèrent le sol simultanément, exactement comme l'avait prévu Galilée.

Comme le contrôleur de la mission le dira plus tard, le résultat fut « rassurant compte tenu à la fois du nombre de témoins oculaires de l'expérience et du fait que le voyage de retour dépendait fortement de la validité de la théorie précisément mise à l'épreuve ». En effet, le voyage dans l'espace serait impossible à planifier sans les équations qui permettent de prévoir la trajectoire du vaisseau spatial soumis à l'attraction de la Terre, du Soleil, de la Lune et des planètes, sans oublier la poussée de ses moteurs.

La version lunaire de l'expérience de Galilée organisée par la NASA est visible sur <http://bit.ly/Galileoprediction>

Après avoir découvert que le poids d'un objet qui tombe n'avait pas d'incidence sur la vitesse de sa chute, Galilée voulut voir s'il pourrait prévoir la durée de la chute. Les objets tombaient trop rapidement pour observer une durée précise à partir d'un point tel que le sommet de la tour de Pise, aussi Galilée décida de faire rouler des boules sur un plan incliné afin d'analyser les variations de vitesse. Il découvrit que si la boule roulait sur une unité de distance en 1 seconde, en 2 secondes elle avait parcouru 4 unités de distance, et en 3 secondes, 9 unités. Il pouvait donc prévoir qu'après 4 secondes, la boule aurait parcouru 16 unités de distance : autrement dit, la distance de chute d'un corps est proportionnelle au carré de la durée de sa chute. En symboles mathématiques :

$$d = \frac{1}{2}gt^2$$

où d est la distance parcourue pendant la chute et t est la durée. Le facteur g , qui est l'accélération due à la gravité, indiquait à Galilée dans quelle mesure la vitesse verticale d'un objet tombant changeait à chaque seconde. Lorsqu'un ballon de football est lâché du haut de la tour de Pise, après 1 seconde, sa vitesse est g , après 2 secondes elle est $2g$, et ainsi de suite. La formule de Galilée fut l'un des premiers exemples d'utilisation d'une équation mathématique pour décrire la nature : ce qu'on appellerait aujourd'hui une loi de la physique.

Ce rôle des mathématiques a révolutionné notre compréhension du monde. Auparavant, les gens utilisaient le langage de tous les jours pour décrire la nature, et cela pouvait être vague : il était possible de dire que quelque chose tombait, mais pas quand cela toucherait le sol. Grâce au langage des mathématiques, il devint possible non seulement de décrire la nature plus précisément, mais aussi de prédire son comportement futur.

Après avoir déterminé ce qu'il arrive à un ballon qu'on laisse tomber, Galilée allait prévoir ce qu'il lui arrive quand on le frappe du pied.

POURQUOI WAYNE ROONEY
RÉSOUT UNE ÉQUATION DU SECOND DEGRÉ
CHAQUE FOIS QUE SA REPRISE
DE VOLÉE ENVOIE LE BALLON DANS LE BUT

« Beckham au coup franc, une reprise de volée parfaitement synchronisée par Rooney... but !!! »

Mais comment Rooney a-t-il réussi un coup pareil ? Vous avez peut-être du mal à le croire, mais Rooney est forcément super fort en mathématiques pour marquer un tel but. Chaque fois qu'il est à la réception d'un coup franc de Beckham, son subconscient résout une autre des équations concoctées par Galilée afin de prévoir où le ballon va aboutir.

Une équation, c'est comme une recette. On prend les ingrédients, on les mélange d'une certaine façon, et on obtient un résultat. Pour écrire l'équation que Rooney va résoudre, il faut à Galilée les ingrédients suivants : la vitesse horizontale u et la vitesse verticale v du ballon au moment de quitter le pied de Beckham, et l'effet de la gravité, lequel est résumé par le nombre g et indique à Rooney la progression seconde par seconde de la vitesse verticale du ballon. La valeur de g dépend de la planète où le match se déroule ; sur la Terre, la gravité augmente la vitesse d'environ 9,8 mètres par seconde (environ 35 km/h par seconde). L'équation de Galilée indique ensuite à Rooney la hauteur du ballon en tout point par rapport à l'endroit où le coup franc a été frappé. Par exemple, si le ballon est à une distance horizontale de x mètres du point où Beckham l'a frappé, alors la hauteur au-dessus du sol sera de y mètres, où y est donné par l'équation

$$y = \frac{v}{u}x - \frac{g}{2u^2}x^2$$

La recette est la série d'instructions mathématiques pour traiter tous ces nombres, et le résultat est la hauteur du ballon à un

certain point de sa trajectoire.

Pour que Rooney puisse déterminer à quelle distance du coup franc il doit se tenir pour reprendre la balle du pied ou de la tête et l'expédier dans les filets, il doit décomposer l'équation en raisonnant à l'envers. Tout d'abord, il opte pour une reprise de la tête. Rooney mesure environ 1,80 mètre, donc le ballon doit être à une hauteur de $y = 1,80$ pour qu'il puisse le frapper (sans sauter). Il connaît les valeurs u , v et g . Prenons quelques nombres approximatifs :

$$u = 20, \quad v = 10, \quad g = 10$$

(Précisons que les vitesses u et v sont en mètres/seconde, et g est en mètres/seconde².)

La seule chose que Rooney ne sait pas, c'est à quelle distance de Beckham il doit se tenir pour bien intercepter le ballon. Mais cette information est en réalité bel et bien codée dans l'équation, elle n'est juste pas visible. L'équation dit que Rooney devrait se tenir à x mètres de Beckham, où x est un nombre qui vérifie :

$$1,8 = \frac{10}{20}x - \frac{10}{2 \times 400}x^2$$

Après simplification, cela donne :

$$x^2 - 40x + 144 = 0$$

Ce type d'équation vous est sans doute familier : c'est une équation quadratique, ou équation du second degré. On peut y penser comme une définition de mot-croisé énigmatique, qui cache la vraie valeur de x .

Aussi étonnant que cela puisse paraître, ce sont les anciens Babyloniens qui, les premiers, commencèrent à résoudre de telles équations. Leurs équations du second degré ne décrivaient pas les trajectoires des ballons de foot, mais apparurent lorsqu'ils firent des relevés topographiques autour de l'Euphrate. Il y a équation du second degré lorsque nous essayons de trouver une quantité qui est multipliée par elle-même. C'est ce qu'on appelle élever au carré, car cela donne l'aire d'un carré ; et c'est lors du calcul de l'aire d'un

terrain que ces équations du second degré furent formulées pour la première fois.

Voici un problème type. Si un champ rectangulaire a une aire de 55 unités carrées, et si un côté mesure six unités de moins que l'autre, quelle est la longueur du côté le plus long ? Si nous appelons x le côté le plus long, alors le problème nous dit que $x \times (x - 6) = 55$ ou, en simplifiant :

$$x^2 - 6x - 55 = 0$$

Mais comment s'y prendre pour démêler ce mystère mathématique ?

Les Babyloniens trouvèrent une méthode élégante : ils découpèrent le rectangle et réagencèrent les morceaux pour obtenir un carré, une forme plus facile à manipuler. Nous pouvons diviser les morceaux de notre champ exactement comme les scribes babyloniens l'auraient fait il y a plusieurs milliers d'années (figure 5.02).

Commencez par découper un petit rectangle mesurant $3 \times (x - 6)$ unités de l'extrémité du rectangle et déplacez-le au bas du rectangle. La forme a changé, mais pas l'aire totale. La nouvelle forme est presque un carré, chaque côté mesurant $x - 3$ unités de long, mais il manque un petit carré de 3×3 dans le coin. Si nous ajoutons ce petit carré, nous augmentons l'aire de la forme de 9 unités. L'aire de ce grand carré est par conséquent de $55 + 9 = 64$. Il nous suffit maintenant de prendre la racine carrée de 64 pour trouver la longueur du côté, qui doit être 8. Mais le côté avait une longueur de $x - 3$, et donc $x - 3 = 8$, c'est-à-dire $x = 11$. Bien que nous n'ayons fait que déplacer des parcelles de terrain imaginaires, derrière ce geste se trouve une méthode générale pour résoudre ces énigmatiques équations du second degré.

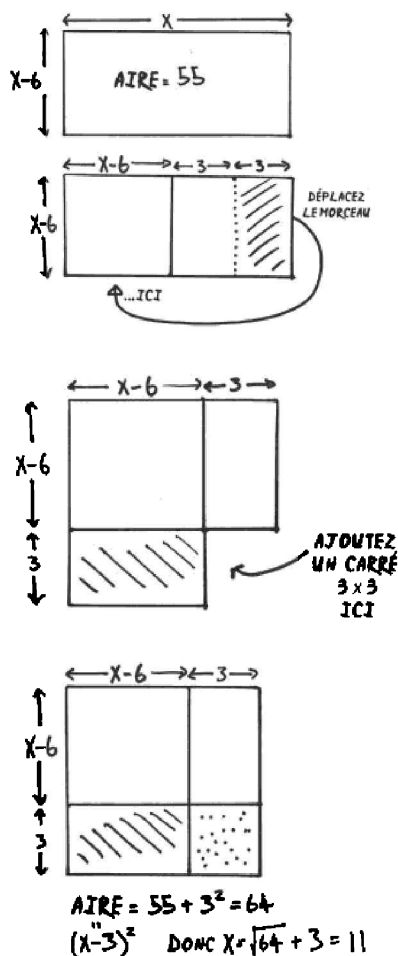


Fig. 5.02 Comment résoudre une équation du second degré en complétant un carré.

Après la naissance de l'algèbre, au IX^e siècle en Irak, il devint possible d'écrire une formule qui exprime la méthode babylonienne. L'algèbre fut créée par le directeur de la Maison de la sagesse à Bagdad, un dénommé Muhammad ibn-Musa al-Khwarizmi. C'est de son nom qu'est issu le mot algorithme. La Maison de la sagesse était alors un centre intellectuel important ; il attirait des érudits du monde entier venus étudier de nombreuses disciplines : astronomie, médecine, chimie, zoologie, géographie, alchimie, astrologie et mathématiques. Les érudits musulmans recueillaient et traduisaient beaucoup de textes anciens, ce qui permit de les préserver pour la postérité — sans eux, nous n'aurions peut-être jamais rien connu des anciennes cultures grecque, égyptienne, babylonienne ou indienne. Mais les érudits de

la Maison de la sagesse ne se contentaient pas de traduire les mathématiques d'autrui. Ils voulaient créer leurs propres mathématiques et faire avancer le sujet.

La curiosité intellectuelle était activement encouragée dans les premiers siècles de l'Empire islamique. Le Coran enseignait que la connaissance du monde rapprochait les gens de la connaissance du sacré. De fait, l'islam exigeait des compétences mathématiques, car les dévots musulmans devaient calculer les heures de prières et connaître la direction de La Mecque pour prier.

L'algèbre d'al-Khwarizmi révolutionna les mathématiques. L'algèbre est un langage qui explique les régularités derrière le comportement des nombres, et sa grammaire sous-tend la manière dont les nombres interagissent. Elle fonctionne un peu comme un code d'exécution d'un programme qui s'applique quels que soient les nombres introduits. Les anciens Babyloniens avaient conçu une méthode astucieuse pour résoudre certaines équations du second degré, mais ce fut la formulation algébrique d'al-Khwarizmi qui aboutit en définitive à une recette pouvant être utilisée pour résoudre toute équation du second degré, quelle qu'elle soit.

Chaque fois que l'on rencontre une équation du second degré $ax^2 + bx + c = 0$, où a , b et c sont des nombres, alors l'astuce géométrique peut être convertie en une formule avec x d'un côté et, de l'autre, une recette combinant les nombres a , b et c :

$$x = \frac{-b + \sqrt{b^2 - 4ac}}{2a}$$

C'est cette formule qui permet à Rooney de résoudre l'équation régissant la trajectoire du ballon et d'en déduire à quelle distance se placer. Quand nous l'avons laissé, il savait qu'il devait se tenir à x mètres du point de frappe, où :

$$x^2 - 40x + 144 = 0$$

Grâce à l'algèbre, il sait qu'il devra se tenir à 36 mètres de Beckham pour intercepter le ballon de la tête.

Comment a-t-il fait ? Eh bien, dans l'équation du second degré contrôlant le coup franc de Beckham, $a = 1$, $b = -40$ et $c = 144$. Donc la formule pour résoudre cette équation nous dit que Rooney doit se placer à une distance de Beckham de :

$$x = \frac{40 + \sqrt{1,600 - 4 \times 144}}{2} = 20 + \frac{\sqrt{1,024}}{2} = 20 + 16$$

$$= 36 \text{ mètres}$$

Par ailleurs, comme -32 est aussi la racine carrée de $1\,024$, nous obtenons une autre solution : $x = 4$ mètres. C'est le point où le ballon amorce son ascension ; Rooney devra attendre que le ballon commence à descendre. Parce qu'il y a toujours une racine carrée négative et une autre positive, cette formule donne toujours deux solutions. Pour indiquer cela, l'équation présente parfois un signe $\pm$ au lieu d'un $+$ devant le symbole de la racine carrée.

Bien entendu, Rooney procède de manière bien plus intuitive : vous l'imaginez faisant 90 minutes de calcul mental ? Mais on voit par là que le cerveau humain est pour ainsi dire programmé par l'évolution pour faire des prévisions.

POURQUOI LE BOOMERANG REVIENT-IL ?

Il arrive d'étranges choses aux objets quand ils tournent. Quand vous frappez un ballon de football de côté, il décrit une courbe dans l'air ; et quand vous lancez en l'air une raquette de tennis, elle tourne toujours avant que vous ne la rattrapiez. Un gyroscope en rotation semble défier la gravité en s'inclinant sur l'horizontale. Mais l'exemple typique de l'étrange comportement d'un objet tournant est la manière dont un boomerang revient vers celui qui l'a lancé.

La dynamique des objets en rotation est d'une complexité telle qu'elle a dérouté bien des générations de savants. Or nous savons désormais que la raison pour laquelle un boomerang revient est liée à deux facteurs distincts. Le premier est associé à la poussée ascendante d'une aile d'avion, et le second est appelé effet gyroscopique. Des équations mathématiques expliquent et prévoient comment la géométrie d'une aile engendre une force qui la pousse vers le haut, contrecarrant la gravité qui tire l'avion vers le bas. Les ailes d'un avion sont dessinées de telle sorte que l'air s'écoule plus vite au-dessus de l'aile qu'en dessous. L'air du dessus

est pressé et poussé plus vite le long de l'aile. C'est le même principe que l'écoulement de l'eau dans un tuyau : si son diamètre se réduit, l'eau s'écoule plus vite.

Une seconde équation, dite de Bernoulli, montre que la vitesse supérieure de l'air sur le haut de l'aile entraîne une pression moindre au-dessus de l'aile, et la vitesse inférieure de l'air au-dessous de l'aile entraîne une pression supérieure à cet endroit. Cette différence de pression crée une force qui soulève l'aile et l'avion, la portance.

Si vous regardez de près un boomerang, vous voyez que chaque pale a la forme d'une aile d'avion, et c'est ce qui le fait tourner. Pour lancer un boomerang en espérant qu'il reviendra, vous devez le lancer en position verticale de telle sorte que (si on le considère comme un avion) l'aile droite soit en haut et l'aile gauche en bas. La même force (ou portance) qui soulève l'aile d'un avion dirige le boomerang vers la gauche.

Mais il se passe ici quelque chose d'un peu plus subtil. Si le boomerang se comportait uniquement comme un avion, la force l'enverrait simplement vers la gauche, sans le faire revenir. S'il revient, c'est que son lancement lui imprime une rotation qui, grâce à l'effet gyroscopique, provoque le changement de direction constant de la force qui le pousse vers la gauche ; il en résulte que le boomerang est poussé le long de l'arc d'un cercle.

Quand je lance le boomerang, la pale supérieure tourne vers l'avant et la pale inférieure vers l'arrière. La pale avançant, en haut, est comme l'aile d'un avion, circulant plus vite dans l'air. Sur un avion volant horizontalement, ce mouvement plus rapide accentuerait la poussée verticale. Mais sur un boomerang lancé verticalement, il le fait s'incliner, son sommet penchant dans l'arc supposé de son vol.

C'est là que l'effet gyroscopique entre en jeu. Quand on place un gyroscope tournant sur un socle en position verticale, il se comporte comme une toupie. Mais si on l'incline de telle sorte que son axe de rotation fasse un angle par rapport à la verticale, un phénomène appelé précession se produit : l'axe de rotation lui-même commence à tourner. C'est ce qui arrive au boomerang en rotation. Son axe de rotation est une ligne imaginaire passant par son centre, et comme cet axe tourne, le boomerang est poussé de façon circulaire.

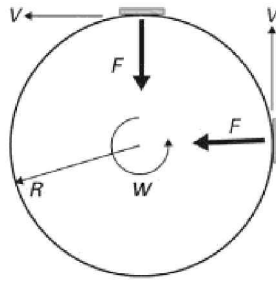


Fig. 5.03 Les forces agissant sur un boomerang. F est la force créée par la poussée vers le haut, V est la vitesse de déplacement du centre du boomerang, R est le rayon de la trajectoire du boomerang et W est le taux de précession.

Quiconque a déjà lancé un boomerang sait qu'il n'est pas facile de le faire revenir. Il faut le lancer de telle sorte que V , la vitesse à laquelle il quitte votre main, et S , le taux de rotation que vous lui imprimez quand vous le lancez, satisfassent à la formule :

$$a \times S = \sqrt{2}V$$

où a est le rayon du boomerang — la distance du centre à l'extrémité. Par un mouvement plus vif du poignet, vous pouvez augmenter S pour appliquer la formule.

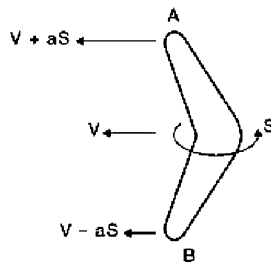


Fig. 5.04 Grâce au taux de rotation, la pale supérieure A du boomerang se déplace plus vite que la pale inférieure B.

L'angle d'inclinaison du boomerang dépend de la différence de vitesse vers l'avant du haut et du bas. Le haut se déplace à la vitesse $V + aS$ tandis que le bas va plus lentement, à $V - aS$, où S est la vitesse angulaire mesurant le taux de rotation du boomerang autour de son centre (voir la figure 5. 04). Il est donc possible de faire varier l'inclinaison du boomerang en changeant les vitesses V

et S , ce qui influencera la vitesse de la précession pendant son arc circulaire à la vitesse V . Si votre boomerang ne revient pas, c'est peut-être que vous ne lui imprimez pas la bonne vitesse de poignet S par rapport à la vitesse de lancement V , et cette équation vous aidera à ajuster votre lancer en conséquence.

Une fois que vous savez comment faire revenir le boomerang, vous vous demandez peut-être : si je le lance plus fort et plus vite, décrira-t-il un arc encore plus grand ? On peut mettre ensemble quelques formules mathématiques et obtenir une équation qui nous donne le rayon de la trajectoire circulaire du boomerang. Une fois de plus, l'équation est une recette au cours de laquelle divers ingrédients définissant le boomerang et son vol sont mélangés afin de donner le rayon. Voici les ingrédients :

J , le moment d'inertie du boomerang. C'est une mesure qui indique combien il est dur de lui imprimer une rotation ; plus le boomerang est lourd, plus J est grand. Le moment d'inertie dépend aussi de la forme du boomerang.

ρ , la densité de l'air que le boomerang traverse.

C_L , le coefficient de portance, un nombre qui détermine la force de la poussée ascendante sur le boomerang, en fonction de sa forme.

π , le nombre 3,14159...

a , le rayon du boomerang.

R , le rayon de la trajectoire du boomerang, est obtenu en mélangeant ces ingrédients d'après la recette :

$$R = \frac{4J}{\rho C_L \pi a^4}$$

Cette équation nous dit que si nous lançons le boomerang plus fort et plus vite, cela ne change pas le rayon parce que la vitesse n'entre pas dans la formule. Mais que se passe-t-il si nous alourdissons le boomerang en collant un peu de Patafix au bout de chaque pale ? Grâce à l'équation, nous savons qu'une augmentation du poids augmentera le moment d'inertie J , ce qui augmentera le rayon R . Par conséquent, un boomerang plus lourd parcourt un plus grand cercle. C'est bon à savoir avant de lancer l'engin dans une pièce d'appartement !

Vous pouvez télécharger un PDF sur la page Web dédiée au livre contenant des instructions pour fabriquer votre propre boomerang.

UN ŒUF PEUT-IL DÉFIER LA GRAVITÉ ?

Prenez un œuf dur, posez-le à plat sur une table et faites-le tourner. Miraculeusement, l'œuf se redresse, semblant défier la gravité. Plus étonnant encore, si vous faites de même avec un œuf cru, la même magie n'opère pas.

Ce n'est qu'en 2002 que les mathématiciens ont pu expliquer ce comportement. L'énergie rotationnelle est convertie, via la friction sur la table, en énergie potentielle qui pousse le centre de gravité de l'œuf vers le haut. Si la table n'a pas de friction ou si elle en a trop, l'effet n'a pas lieu. Une partie de l'énergie transférée vers un œuf cru est absorbée par l'intérieur fluide, et il n'en reste pas assez pour pousser l'œuf en position verticale.

POURQUOI LES PENDULES NE SONT PAS AUSSI PRÉVISIBLES QU'IL Y PARAÎT

C'est Galilée, maître en prédictions fondées sur les mathématiques, qui, le premier, découvrit le secret du tic-tac d'un pendule. On raconte qu'à l'âge de dix-sept ans, alors qu'il assistait à une messe à la cathédrale de Pise, dans un moment d'ennui, il leva les yeux au plafond et remarqua un lustre qui se balançait doucement sous l'effet de la brise qui traversait l'édifice.

Galilée décida de mesurer le temps qu'il fallait au lustre pour osciller d'un côté à l'autre. La montre n'ayant pas encore été inventée, il se servit de son pouls, et eut la grande surprise de découvrir que la durée d'une oscillation complète du lustre ne semblait pas dépendre de l'ampleur du mouvement. Autrement dit, le fait d'augmenter ou de diminuer l'angle du balancement ne change pas essentiellement sa durée. (Je mets le mot « essentiellement » ici pour indiquer que, si l'on creuse un peu plus, les choses se compliquent légèrement.) Quand le vent soufflait plus fort, le lustre parcourait un plus grand arc mais en autant de temps que lorsqu'il bougeait à peine par faible vent.

Cette découverte majeure conduisit à l'utilisation du pendule pour enregistrer le temps qui passe. Lorsqu'on met en route une

horloge à pendule, peu importe la distance latérale de départ, d'autant plus que l'angle du balancier va diminuer progressivement. Mais de quoi dépend la durée de l'oscillation, et peut-on prévoir comment elle changera sous l'effet de l'augmentation du poids ou de l'allongement du pendule ?

Comme le suggère l'expérience de Galilée à la tour de Pise, un pendule plus lourd ne se déplace pas plus vite, et donc son oscillation ne dépend pas de son poids. En revanche, un pendule plus long influence effectivement la durée de l'oscillation. Si l'on multiplie la longueur par 4, la durée double ; par 9, elle triple ; et par 16, elle quadruple.

Encore une fois, une équation peut résumer cette prévision. La durée de l'oscillation T augmente selon la racine carrée de la longueur L :

$$T \approx 2\pi \sqrt{\frac{L}{g}}$$

C'est là en réalité une autre manière d'écrire l'équation formulée par Galilée concernant le lâcher de boules depuis le haut de la tour de Pise : le g est, à nouveau, l'accélération due à la gravité. J'utilise un $\approx$ et non un $=$ parce qu'il s'agit d'une bonne approximation du temps qu'un pendule met pour osciller d'un côté à l'autre. Tant que l'oscillation n'est pas trop grande, il est possible d'utiliser cette équation pour prévoir le comportement du pendule. Mais si l'angle de l'oscillation est important — par exemple, si nous faisons démarrer le pendule presque horizontalement —, le calcul devient alors beaucoup plus compliqué. L'angle affecte la durée de l'oscillation, ce que Galilée n'a pas pu observer dans la cathédrale puisque le lustre ne pouvait pas se balancer si loin. Nous ne voyons pas non plus l'effet dans une horloge de parquet, l'oscillation du pendule y étant très réduite.

Le niveau de mathématiques nécessaire pour trouver l'équation capable de prévoir le comportement d'un pendule avec un grand angle d'oscillation est bien supérieur à ce qui est généralement enseigné dans la discipline. Voici le début de la formule. En fait, elle contient un nombre infini d'éléments qui contribuent au comportement du pendule. θ_0 est l'angle initial du pendule par rapport à la verticale.

$$T \approx 2\pi \sqrt{\frac{L}{g}} \left(1 + \frac{1}{16} \theta_0^2 + \frac{11}{3,072} \theta_0^4 + \dots \right)$$

Mais cela n'est rien par rapport à la prévision du comportement d'un pendule légèrement modifié. Au lieu d'une seule tige rigide qui se balance, imaginez que l'on ajoute un second pendule articulé au bas du premier, comme une sorte de jambe articulée au genou. Prévoir le comportement de ce double pendule est extrêmement difficile. Non pas que les équations soient tellement plus compliquées, mais leurs solutions sont imprévisibles : une modification infime de la position initiale du pendule peut changer radicalement le résultat. En effet, le double pendule est un exemple d'un phénomène mathématique appelé chaos. Mais le double pendule n'est pas seulement un jeu amusant sur ordinateur. Les mathématiques sous-jacentes ont des conséquences potentiellement graves pour l'avenir même de l'humanité.

<http://bit.ly/Myphysicslab> est l'une des nombreuses simulations informatiques en ligne des doubles pendules. Essayez de prévoir si l'élément inférieur passera dans le sens des aiguilles d'une montre ou inversement au travers du pendule du haut. C'est presque impossible. Pour créer votre propre pendule, allez sur <http://bit.ly/DoublePendulum>

LE SYSTÈME SOLAIRE VA-T-IL VOLER EN ÉCLATS ?

Depuis que Galilée s'est intéressé à la chute des boules et à l'oscillation des pendules, des centaines de milliers d'équations qui prédisent les phénomènes naturels ont été formulées par les mathématiciens. Ces équations constituent les fondements de la science moderne ; ce sont les lois de la nature. C'est grâce aux mathématiques que le monde technologique complexe d'aujourd'hui existe. Les ingénieurs s'appuient sur des équations pour s'assurer que leurs ponts ne s'effondreront pas et que les

avons voleront. Après avoir lu ce qui précède, vous pourriez croire qu'il est facile de prévoir le futur, mais ce n'est pas toujours aussi simple — comme l'a découvert le mathématicien français Henri Poincaré (1854-1912).

En 1885, le roi Oscar II de Suède et de Norvège offrit un prix de 2500 couronnes à quiconque pourrait affirmer mathématiquement que le système solaire continuerait à tourner comme une horloge, ou alors qu'à un certain moment, il se pourrait que la Terre s'éloigne du Soleil à l'infini. Poincaré, s'estimant capable de trouver la réponse, commença ses recherches.

Pour analyser un problème compliqué, les mathématiciens ont pour habitude de simplifier les données du problème dans l'espoir d'en simplifier la résolution. Ainsi, au lieu de démarrer avec toutes les planètes du système solaire, Poincaré considéra un système composé de deux corps seulement. Isaac Newton avait déjà prouvé que leurs orbites étaient alors stables : les deux corps circulent en orbites elliptiques l'un autour de l'autre, selon un schéma qui se reproduit périodiquement.

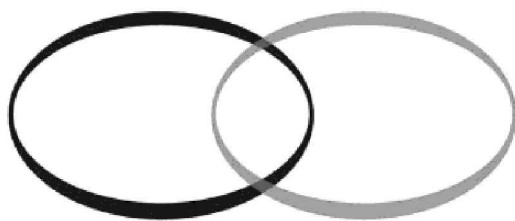


Fig. 5.05

Partant de là, Poincaré commença à explorer ce qu'il advient quand on ajoute une autre planète à l'équation. Malheureusement, dès qu'il y a trois corps dans un système, par exemple la Terre, la Lune et le Soleil, il devient très compliqué de savoir si leurs orbites sont stables. Au point d'ailleurs de déconcerter jusqu'au grand Newton. La difficulté réside dans le fait qu'il y a maintenant 18 ingrédients à combiner : les coordonnées exactes de chaque corps (un point, ce sont trois coordonnées) et leurs vitesses. Newton lui-même écrivit que « considérer simultanément toutes ces causes de mouvement et définir ces mouvements par des lois exactes permettant un calcul facile dépasse, sauf erreur de ma part, la force de tout esprit humain ».

Le mémoire de Poincaré, « Sur le problème des trois corps et les

équations de la dynamique », fit l'unanimité du jury et aurait dû être publié en octobre 1889. Mais grâce aux questions du jeune mathématicien Lars Phragmen, chargé par le président du jury Mittag-Leffler de la lecture détaillée des mémoires, Poincaré s'aperçut qu'une erreur subsistait dans son exposé. En décembre, il annonça à Mittag-Leffler que son manuscrit nécessitait de sérieux changements. Publier en l'honneur du roi un mémoire erroné aurait été un affront à la Couronne suédoise ; Poincaré récupéra donc discrètement les premiers tirages déjà en circulation et régla les frais de l'impression (c'était plus que la récompense du prix). La version révisée fut prête en avril 1890.

La rectification de l'erreur de Poincaré l'a mené à une découverte capitale, celle de la « dépendance sensitive des conditions initiales », plus tard appelée théorie du chaos. Comme souvent en mathématiques, un fourvoiement peut conduire à d'intéressantes avancées. Poincaré écrivit un article expliquant que des minimes changements pouvaient soudain faire voler en éclats un système apparemment stable.

Poincaré avait trouvé que, même dans l'univers réglé comme une horloge de Newton, des équations simples peuvent produire des résultats extrêmement complexes. Nous ne sommes pas là dans les mathématiques de l'aléatoire, des probabilités, mais face à un système que les mathématiciens appellent déterministe : il est régi par des équations mathématiques classiques, et pour un ensemble fixé de conditions de départ, l'aboutissement sera le même. Un système chaotique reste déterministe, mais un très petit changement des conditions de départ peut conduire à un résultat très différent.

Voici un exemple à petite échelle qui est un bon modèle du système solaire. Nous posons sur le sol trois aimants : un noir, un gris et un blanc. Au-dessus, nous installons un pendule magnétique qui se balance en toute liberté. Le pendule sera attiré par les trois aimants, et oscillera entre eux avant de se stabiliser. À l'extrémité du pendule se trouve une cartouche d'où s'écoule de la peinture. Nous lançons l'oscillation du pendule et la peinture trace sa trajectoire. En réalité, nous tentons de simuler un astéroïde traversant à toute allure un système solaire dont trois planètes l'attirent : finalement, l'astéroïde heurtera l'une d'elles.

Aussi extraordinaire que cela puisse paraître, il est presque impossible de répéter deux fois l'expérience en obtenant le même tracé de peinture. Même en s'évertuant à déclencher le pendule à la même position et dans la même direction, on constate que la

peinture trace un chemin complètement différent et finit chaque fois attirée par un aimant différent. La figure 5.06 montre trois parcours qui démarrent à peu près de la même façon mais s'arrêtent sur des aimants différents.

Les équations qui contrôlent la trajectoire de l'aimant sont chaotiques, et un changement infime de la position de départ modifie radicalement le résultat. C'est la signature du chaos.

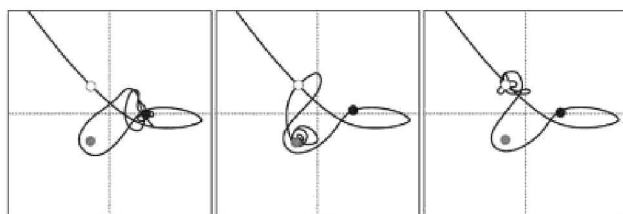


Fig. 5.06 Un petit changement de la position initiale du pendule peut lui faire suivre un parcours complètement différent entre les trois aimants (représentés par les trois petits ronds blanc, gris et noir).

Nous pouvons utiliser un ordinateur pour produire une image montrant par quel aimant le pendule sera attiré (figure 5.07). Les aimants sont placés aux centres de trois grands blocs de couleur en forme de vase. Si vous lancez le pendule au-dessus d'une zone noire, il finira par se stabiliser au-dessus de l'aimant noir. De même, si vous le lancez au-dessus d'une région grise ou blanche, il s'arrêtera sur l'aimant de même couleur. Vous pouvez voir des zones de cette image dans lesquelles un faible déplacement du point de départ du pendule n'affectera pas sensiblement le résultat. Par exemple, si vous démarrez près de l'aimant noir, le pendule finira probablement son trajet sur celui-ci. Mais il y a d'autres zones où les couleurs changent rapidement sur de courtes distances.

C'est un exemple d'une forme que la nature adore : la forme fractale. Les fractales sont la géométrie du chaos, et si vous faisiez un gros plan sur l'une des zones de cette image, vous verriez le même niveau de complexité, comme nous l'avons étudié page 140. C'est cette complexité qui rend le mouvement du pendule si difficile à prévoir, malgré la simplicité des équations qui le décrivent.

Et si l'enjeu n'était pas juste le point d'arrêt de l'oscillation d'un pendule, mais l'avenir du système solaire ? Peut-être qu'une petite perturbation due à un vilain astéroïde causera un changement minime mais suffisant pour disloquer ledit système. Cela semble s'être produit dans le proche système solaire de l'étoile Upsilon Andromedae. Les astronomes pensent que l'étrange comportement des planètes existantes est la preuve d'une catastrophe au cours de laquelle l'une des planètes originelles en orbite autour de l'étoile aurait été éjectée après que quelque chose a perturbé les orbites auparavant stables. La même chose pourrait-elle se produire sur notre planète ?

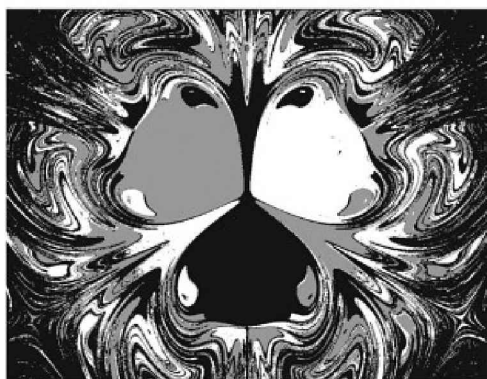


Fig. 5.07 Cette image générée par ordinateur illustre le comportement du pendule en mouvement au-dessus des aimants.

Juste pour se rassurer, les scientifiques ont récemment utilisé des superordinateurs pour essayer de répondre à la question qui avait mis Poincaré en échec : la Terre court-elle vraiment le risque de s'éloigner à jamais dans l'espace ? Ils ont simulé les orbites réelles, passées et futures, des planètes et ont conclu qu'il y avait 99 % de chances qu'elles continuent d'évoluer sagement dans leurs orbites pendant encore 5 milliards d'années (époque à laquelle le Soleil, s'étant transformé en géante rouge, aura absorbé le système solaire interne). Mais cela laisse 1 % de chances pour une issue légèrement plus intéressante... au moins du point de vue mathématique.

Il s'avère que les planètes intérieures rocheuses — Mercure, Vénus, la Terre et Mars — ont des orbites moins stables que les géantes gazeuses : Jupiter, Saturne, Uranus et Neptune. Livrées à leurs propres mouvements, ces grosses planètes auraient un avenir

remarquablement stable. C'est la minuscule Mercure qui est capable de provoquer un effondrement catastrophique du système solaire.

Des simulations informatiques révèlent qu'une étrange résonance entre Mercure et Jupiter pourrait évoluer de telle sorte que l'orbite de Mercure commencerait à croiser celle de sa plus proche voisine, Vénus. D'où un risque de collision gigantesque entre Vénus et Mercure, qui désintégrerait le système solaire. Mais cela se produira-t-il ? Nous ne le savons pas. Le chaos rend toute prévision très difficile.

COMMENT UN PAPILLON PEUT-IL TUER DES MILLIERS DE PERSONNES ?

Il n'y a pas que le système solaire qui soit chaotique. Beaucoup de phénomènes présentent des traits chaotiques : le comportement de la Bourse, l'apparition progressive d'une vague monstrueuse en mer, le battement du cœur. Mais le système chaotique qui affecte le plus la vie de chacun est la météorologie. Nous ne nous préoccupons pas beaucoup de savoir si la Terre sera encore dans l'orbite du Soleil dans un milliard d'années ; en revanche nous voulons savoir s'il fera beau la semaine prochaine et, peut-être aussi, si le climat dans vingt ans sera très différent de celui d'aujourd'hui.

La prévision météorologique a toujours été un peu de la magie noire, même si une partie du folklore en la matière s'est révélée juste. « Rouge au soir, beau temps en espoir » est un fait car les rayons du soleil ont rougi en traversant une vaste zone de ciel clair vers l'ouest. Et comme les systèmes météorologiques en Europe arrivent généralement de l'ouest, cela annonce en effet du beau temps.

Les météorologues contemporains disposent d'une multitude de données allant des mesures des stations météo en mer aux images et informations captées par satellite. Et ils ont des équations extrêmement précises pour décrire comment les masses d'air qui se heurtent dans l'atmosphère interagissent pour créer des nuages, du vent et de la pluie. Dès lors que nous avons les équations mathématiques qui régissent la météo, il devrait être assez simple

de les soumettre à un ordinateur avec les données météo du jour et d'en déduire le temps qu'il fera la semaine prochaine, non ?

Hélas, même les superordinateurs d'aujourd'hui ne permettent pas de prévoir avec certitude la météo dans deux semaines. Nous ne savons pas précisément le temps qu'il va faire aujourd'hui, et encore moins dans les jours qui viennent. Même les meilleures stations météorologiques ne fournissent qu'une précision limitée. Nous ne connaissons jamais la vitesse exacte de chaque particule dans l'air, la température précise en chaque point de l'espace, ni la pression au pascal près sur toute la planète. Et la moindre variation de l'un de ces facteurs peut modifier radicalement la prévision. D'où l'expression « l'effet papillon » : le battement d'ailes d'un papillon crée dans l'atmosphère de minuscules changements qui peuvent entraîner la formation d'une tornade ou d'un ouragan à l'autre bout du monde, provoquant des ravages, des pertes humaines et des dégâts matériels considérables.

C'est pour cette raison que les météorologues travaillent sur plusieurs prévisions simultanées en prenant pour base les relevés des satellites qu'ils modifient afin de créer les différents scénarios. Parfois, toutes les prévisions aboutissent à peu près aux mêmes résultats, et les météorologues peuvent alors en déduire avec une certaine confiance que la météo — quoique connue pour être chaotique — sera stable pendant une ou deux semaines. D'autres fois, les prévisions diffèrent complètement, et les mêmes spécialistes admettent leur incapacité à prévoir exactement le temps des prochains jours.

Lorsque notre pendule chaotique oscillait entre les trois aimants, il y avait, dans l'image prévoyant son comportement, des zones où un petit changement de la position initiale du pendule ne le ferait pas aboutir sur un aimant différent. Il en va de même avec la météorologie. Imaginez que la grande zone noire de l'image soit la météo dans un désert : il y fera toujours chaud, même si un papillon bat des ailes frénétiquement. Même chose pour l'Arctique où l'aimant reste dans une zone blanche. Mais pour le Royaume-Uni ou la France, la météo ressemble au pendule démarrant dans un endroit où le moindre décalage de sa position modifie rapidement les couleurs de l'image.

Si nous connaissions les positions et vitesses précises de toutes les particules dans l'univers, nous pourrions prévoir l'avenir avec certitude. En réalité, si l'une de ces positions de départ est un tant soit peu faussée, l'avenir peut s'avérer complètement différent. L'univers est peut-être réglé comme une horloge, mais nous ne

connaîtrons jamais les positions des roues dentées avec assez de précision pour tirer parti de sa nature déterministe.

PILE OU FACE ?

Lors du Championnat d'Europe de football de 1968, l'épreuve des tirs au but n'existait pas encore en cas de match nul. Aussi, quand la demi-finale entre l'Italie et l'Union soviétique se termina sur un score vierge après prolongations, le finaliste fut tiré à pile ou face. Depuis l'époque romaine, une pièce de monnaie est un moyen universellement reconnu pour régler un différend. Après tout, quand elle tourne en l'air il est impossible de savoir de quel côté elle va retomber. Mais est-ce si vrai ?

Théoriquement, si vous connaissiez précisément la position de la pièce, la vitesse de rotation et le moment de l'atterrissage, vous pourriez en déduire le résultat. Mais, à l'instar du climat, la moindre variation de l'un de ces facteurs pourrait-elle changer complètement le résultat ? Persi Diaconis, mathématicien à l'université Stanford, Californie (également connu comme magicien professionnel), a voulu savoir si le lancer de pièce est aussi imprévisible qu'il y paraît. Si les conditions sont les mêmes à chaque lancer, les calculs aboutiront toujours au même résultat. Mais la marque du chaos est-elle cachée dans le jet de la pièce ? Qu'advient-il si nous changeons très légèrement ces conditions initiales : les changements sont-ils amplifiés au point qu'il est impossible de prévoir si la pièce va donner pile ou face ?

Aidé d'amis ingénieurs, Diaconis a construit une machine mécanique lanceuse de pièces capable de reproduire indéfiniment les conditions du lancer. Bien sûr, il y aurait de très légères différences entre deux lancers, mais produiraient-elles des résultats largement différents, comme le pendule se balançant entre trois aimants ? Diaconis a constaté qu'à chaque essai avec sa machine lanceuse, la pièce tombait du même côté. Il s'est alors entraîné à lancer lui-même la pièce de façon identique à chaque fois, de manière à obtenir 10 faces d'affilée. Évitez de jouer à pile ou face avec ce genre d'individu.

Mais qu'en est-il du lanceur λ dont deux jets successifs ne seront jamais identiques ? Diaconis s'est demandé si un biais restait possible. Pour commencer son analyse mathématique, il lui

fallait un expert en objets tournants. Il l'a trouvé en la personne de Richard Montgomery, rendu célèbre pour avoir apporté la preuve du théorème du chat, une théorie qui explique pourquoi un chat lancé ou tombant sous n'importe quel angle retombera toujours sur ses pattes. Avec la statisticienne Susan Holmes, ils ont montré qu'une pièce lancée d'un coup de pouce a tendance à tomber d'un certain côté.

Pour convertir la théorie en données chiffrées, il leur fallait analyser de très près le déplacement en l'air d'une pièce en rotation. Avec une caméra numérique ultra-rapide, prenant 10 000 images par seconde, ils ont saisi le déplacement d'une pièce et introduit ces données dans leur modèle théorique. Leur constatation peut surprendre : il y a bien un biais lors d'un vrai lancer de pièce. Léger, certes : à 1 %, la pièce retombait avec la même face sur le dessus qu'au moment du coup de pouce. La raison semble liée à la physique du boomerang ou du gyroscope. Apparemment, la pièce en rotation connaît le même phénomène de précession qu'un gyroscope, et donc passe un peu plus de temps en l'air avec la face initialement dirigée vers le haut. La différence est négligeable pour un seul lancer, mais pourrait se révéler très significative à long terme.

S'il est une entreprise qui s'intéresse au long terme, c'est bien le casino, dont le bénéfice dépend des probabilités sur le long terme. À chaque jet de dés ou tour de roulette, les casinos comptent sur votre incapacité à prévoir le résultat. Pourtant, comme pour le lancer de pièce, si vous connaissiez précisément les positions de départ du plateau de la roulette et de la bille, et leurs vitesses initiales, vous pourriez théoriquement, grâce à la physique newtonienne, savoir où la bille s'arrêtera. Si le plateau de la roulette démarre exactement dans la même position et à la même vitesse, et si le croupier lance la boule exactement de la même manière à chaque fois, celle-ci aboutira au même endroit. Le problème est identique à celui découvert par Poincaré : un changement même infime des positions de départ et des vitesses du plateau et de la bille peuvent modifier grandement le point d'arrivée de la bille. Et il en va de même avec les dés.

Mais cela ne signifie pas que les mathématiques ne peuvent pas nous aider à réduire la plage d'arrivée de la bille. On peut observer quelques rotations de la boule avant de faire son jeu, et donc analyser sa trajectoire et prévoir sa destination finale. C'est précisément ce qu'ont fait trois Européens de l'Est : une femme hongroise décrite comme « chic et très belle » et deux hommes

serbes « élégants ». Ils ont eu recours aux mathématiques pour faire un malheur à la roulette du casino du Ritz de Londres, en mars 2004.

Au moyen d'un scanner laser caché dans un téléphone mobile relié à un ordinateur, ils ont enregistré la vitesse du plateau par rapport à la bille durant deux rotations. L'ordinateur en a déduit une zone de six nombres où la bille devait aboutir. Pendant la troisième rotation du plateau, les joueurs ont placé leurs mises. Les chances de gagner étant passées de 1 à 37 à 1 à 6, le trio a misé sur les six nombres en question... et a empoché 100 000 euros dès le premier soir... pour passer à 1,2 million d'euros le lendemain. Arrêtés et placés en liberté provisoire pendant neuf mois, ils ont finalement été libérés et autorisés à conserver leurs gains. En effet, les juges sont parvenus à la conclusion qu'ils n'avaient en rien trafiqué le plateau.

Ces joueurs savaient que, bien qu'il y ait du chaos dans un plateau de roulette, une légère modification des positions de départ de la bille et du plateau n'entraîne pas toujours un vrai changement. C'est sur cela que comptent les météorologues pour leurs prévisions. Parfois, en faisant tourner leurs modèles informatiques, ils constatent que le fait de changer les conditions météorologiques aujourd'hui n'a pas d'effet sensible sur les prévisions. L'ordinateur de nos joueurs a fait de même en passant au crible des milliers de scénarios différents pour voir où la bille pourrait finir sa course. Il n'a pas pu fournir la position exacte, mais une suite de six nombres, bien suffisante pour retourner le destin en faveur des joueurs.

De ce qui précède, vous pourriez déduire que la nature se décompose en problèmes simples et prévisibles — comme une boule tombant du sommet de la tour de Pise — et en problèmes chaotiques et difficiles à prévoir — comme la météo. Mais ce n'est pas aussi tranché. Parfois, ce qui semble à première vue aisément prévisible peut devenir chaotique dès lors qu'une seule petite chose change ne serait-ce que de manière infime.

QUI A TUÉ TOUS LES LEMMINGS ?

Voilà quelques années, des écologistes ont remarqué que, tous les quatre ans, le nombre de lemmings semble diminuer dans des

proportions inquiétantes. Selon la théorie en vogue, ces rongeurs de l'Arctique gravissaient une falaise abrupte et se précipitaient dans le vide pour s'écraser sur les rochers en contrebas. En 1958, l'unité d'histoire naturelle de Walt Disney Production a inclus une séquence de ce suicide collectif dans un film à succès, *Le Désert de l'Arctique*. Le réalisme de la scène était si convaincant que le mot « lemming » en est venu à désigner quiconque suit aveuglément les autres sans peser les risques potentiels — comme les « moutons de Panurge » en France. Le comportement de ces animaux a même inspiré un jeu vidéo qui consistait à sauver les lemmings de cette marche folle vers l'abîme.

Dans les années 1980, on a révélé que l'équipe de tournage du film avait truqué toute la séquence. D'après un documentaire de la télévision canadienne, les lemmings, achetés spécialement pour le tournage, refusaient de sauter au signal et furent « aidés » par les membres de l'équipe. Mais si ce n'est pas le suicide de masse qui est la cause de cette baisse soudaine du nombre de lemmings tous les quatre ans, quelle est donc l'explication ?

Pour voir la séquence du film *Le Désert de l'Arctique*, rendez-vous sur <http://bit.ly/Whitewilderness>

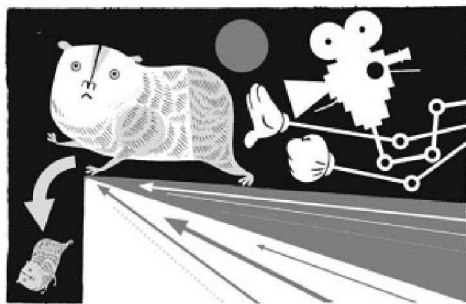


Fig. 5.08

Là encore, il se trouve que les mathématiques ont la réponse. Une simple équation nous indique combien de lemmings il y aura d'une saison à la suivante. Pour commencer, nous partons du principe que, compte tenu de facteurs environnementaux tels que l'alimentation et les prédateurs, il y a une population maximale acceptable. Nous l'appellerons N . Nous appellerons L le nombre de

lemmings survivants de la saison précédente, et après les naissances de la nouvelle saison, la population s'élève à K lemmings, dont une certaine proportion ne survivra pas. La proportion qui meurt est $\frac{L}{N}$, soit le nombre de lemmings de la saison précédente divisé par la population maximale possible.

Donc $K \times \frac{L}{N}$ meurent, laissant

$$K - \frac{K \times L}{N}$$

lemmings à la fin de cette saison. Pour simplifier nos calculs, disons que la population maximale est de $N = 100$.

Quoique simple, cette équation donne des résultats surprenants. Commençons par voir ce qui se passe si la population double à chaque printemps, de sorte que $K = 2L$. De ce nombre de lemmings, $2L \times \frac{L}{100}$ mourront. Supposons qu'il y a 30 lemmings

la première saison. L'équation prévoit qu'à la fin de la deuxième saison il y aura $60 - \left(60 \times \frac{30}{100}\right) = 42$ lemmings. Leur nombre continue d'augmenter jusqu'à ce qu'il y en ait 50 à la quatrième saison.

À partir de là, le nombre de lemmings qui survivent chaque saison se stabilise à 50. Ce qui est étonnant, c'est que, quelle que soit la population au début de la première saison, le nombre de lemmings restants à la fin de chaque saison suivante sera la moitié du nombre maximum et le demeurera. Ainsi, quand on atteint 50 lemmings, le nombre double pour atteindre 100 au cours de la saison suivante, mais à la fin de la saison $100 \times \frac{50}{100} = 50$ seront morts, laissant à nouveau une population de 50 lemmings (figure 5.09).

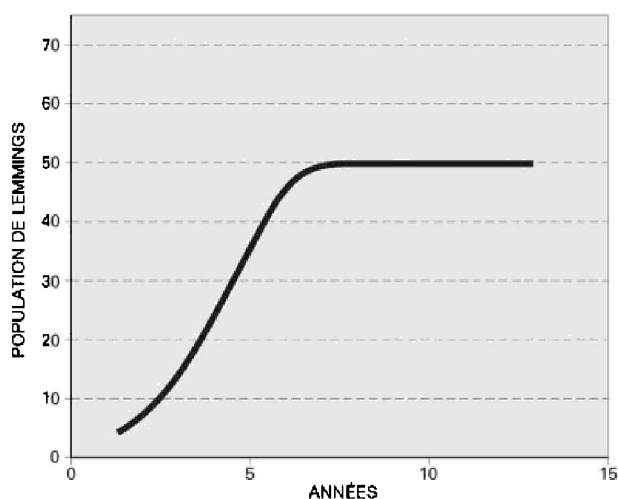


Fig. 5.09 Si le nombre de lemmings double à chaque printemps, la population atteint une valeur stable quel que soit leur nombre initial.

Et si les lemmings étaient plus féconds ? Si leur nombre fait un peu plus que tripler d'une saison à l'autre, on remarque que la population ne se stabilise pas mais oscille entre deux valeurs. Si le nombre de survivants à la fin d'une saison est très élevé, il diminue la saison suivante.

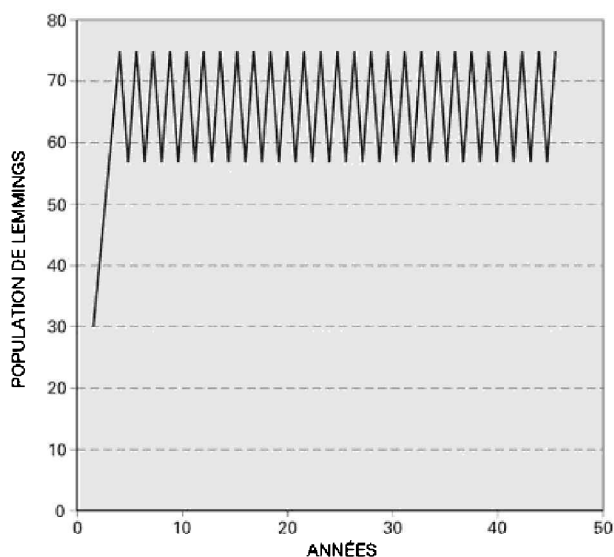


Fig. 5.10 Si le nombre de lemmings triple au printemps, la population commence à osciller.

Lorsque les lemmings sont encore plus féconds, la population commence à fluctuer d'une manière étrange. Si la population augmente d'un facteur 3,5, le nombre total de lemmings oscille entre quatre valeurs, en répétant ce schéma toutes les quatre saisons. (Le facteur précis à partir duquel les quatre valeurs apparaissent pour la première fois est $1 + \sqrt{6}$, soit environ 3,449.) Et c'est là que nous constatons que, durant l'une de ces quatre années, le nombre de lemmings peut chuter sensiblement non pas à cause d'un suicide collectif, mais à cause des mathématiques.

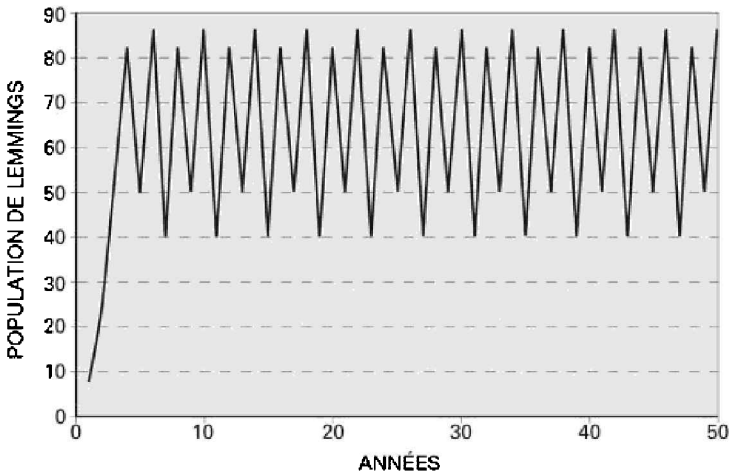


Fig. 5.11 Lorsque le nombre de lemmings augmente au printemps d'un facteur 3,5, la population oscille entre quatre valeurs différentes.

Le changement réellement intéressant dans cette dynamique se produit quand le nombre de lemmings augmente d'un facteur juste supérieur à 3,5699. Dans ce cas, leur nombre varie capricieusement d'une saison à l'autre, sans aucune logique. Bien que l'équation qui détermine la population soit simple, elle a commencé à produire des résultats chaotiques. Si l'on change le nombre initial de lemmings, la dynamique démographique est complètement différente. Une fois dépassé le seuil où apparaît le chaos, 3,5699, la variation démographique est presque impossible à prévoir. L'équation du suivi du nombre de lemmings peut démarrer de façon très prévisible, mais soudain un léger changement dans le taux de fécondité peut entraîner le chaos.

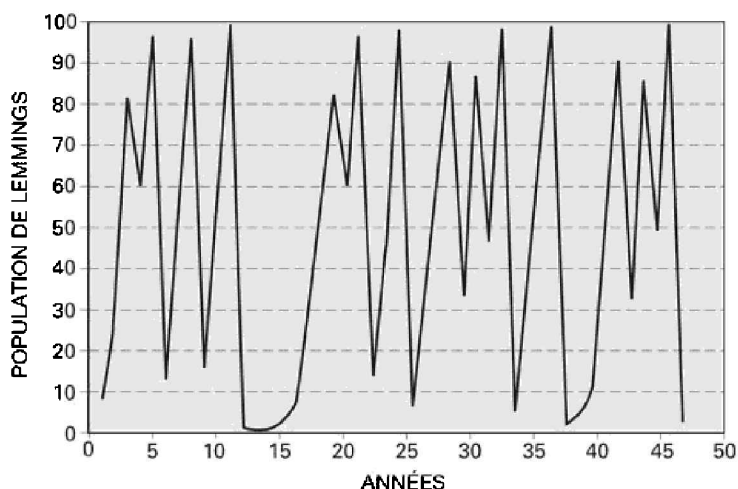


Fig. 5.12 Quand le nombre de lemmings augmente au printemps d'un facteur 3,5699 ou plus, les écarts démographiques deviennent chaotiques.

LA VIE EST UN JEU DE POISSONS

C'est un jeu pour deux personnes. Téléchargez le PDF à partir de la page Web du livre et découpez les dix poissons et l'aquarium. Le jeu étudie la variation du nombre de poissons sur dix saisons. Chaque poisson correspond à une saison. Sur le côté des poissons se trouve une boîte dans laquelle on peut noter le nombre de poissons dans l'aquarium correspondant à cette saison. L'aquarium peut accepter un maximum de 12 poissons. Les poissons survivent un an, durant lequel ils ont un certain nombre de petits, ou alevins.

Lancez deux dés. Le nombre de poissons initial dans l'aquarium est la valeur des dés moins un (donc, compris entre 1 et 11). Appelons ce nombre N_0 . Le premier joueur choisit un nombre, K , entre 1 et 50. Cela déterminera le nombre d'alevins de chaque poisson. S'il y a N_0 poissons dans l'aquarium au début, durant la première année ils donneront naissance à $(\frac{K}{10}) \times N_0$ poissons. Le nombre de poissons est

donc multiplié par $\frac{K}{10}$, un nombre situé entre 0,1 et 5.

Tous les nouveaux poissons ne survivront pas. S'il y avait N poissons dans l'aquarium à la fin de l'année précédente, à la fin de l'année suivante le nombre sera de

$$\frac{K}{10} \times N \times \left(1 - \frac{N}{12}\right)$$

Vous devez arrondir à l'unité supérieure ou inférieure pour obtenir un nombre entier de poissons (4,5 est arrondi à 5).

Laissez l'aquarium « vivre » pendant dix ans. Le premier joueur marque le nombre de poissons dans l'aquarium à la fin des années impaires, et le second fait de même pour les années paires.

Soit N_i le nombre de poissons dans l'année i .

Le joueur 1 marque $N_1 + N_3 + N_5 + N_7 + N_9$

Le joueur 2 marque $N_2 + N_4 + N_6 + N_8 + N_{10}$

En notant les informations sur la forme découpée du poisson, vous pouvez suivre la population d'une année à l'autre. Si tous les poissons meurent à un moment donné, alors le joueur 1, qui a choisi le multiplicateur K , perd automatiquement.

Voici un exemple. Les joueurs lancent les deux dés et obtiennent 4. Il y a donc trois poissons dans l'aquarium pour commencer : $N_0 = 3$. Le joueur 1 choisit $K = 20$. Le nombre de poissons à la fin de l'année 1 est donc :

$$N_1 = \frac{K}{10} \times N_0 \times \left(1 - \frac{N_0}{12}\right) = 2 \times 3 \times \left(1 - \frac{3}{12}\right) = 4,5 \approx 5$$

L'année 2, il y a :

$$N_2 = \frac{K}{10} \times N_1 \times \left(1 - \frac{N_1}{12}\right) = 2 \times 5 \times \left(1 - \frac{5}{12}\right) = 5\frac{5}{6} \approx 6$$

poissons, et l'année 3, il y a :

$$N_3 = \frac{K}{10} \times N_2 \times \left(1 - \frac{N_2}{12}\right) = 2 \times 6 \times \left(1 - \frac{6}{12}\right) = 6$$

poissons. Le nombre de poissons est maintenant stabilisé parce que 6 se répète quand il est mis dans la formule. Donc :

le joueur 1 marque $5 + 6 + 6 + 6 + 6 = 29$ poissons

le joueur 2 marque $6 + 6 + 6 + 6 + 6 = 30$ poissons
et le joueur 2 gagne. Voyez ce qui se passe en faisant varier le multiplicateur K .

Puisque nous arrondissons les nombres à l'unité supérieure ou inférieure, le jeu est moins subtil que le modèle chaotique qui a exterminé les lemmings.

Pour accompagner ce jeu d'un simulateur d'aquarium en ligne, visitez <http://bit.ly/Tanksim>.

Dans la version du jeu de cette simulation, le nombre de poissons affiché a été arrondi à l'unité supérieure ou inférieure, mais la fraction restante est introduite dans la formule pour l'année suivante. Par exemple, si vous définissez $K = 27$ et $N_0 = 3$,

$N_1 = 6,075$, arrondi à 6 poissons

$N_2 = 8,09873$, arrondi à 8 poissons

$N_3 = 7,10895$, arrondi à 7 poissons

$N_4 = 7,8233$, arrondi à 8 poissons

$N_5 = 7,352$, arrondi à 7 poissons

$N_6 = 7,68872$ arrondi à 8 poissons

$N_7 = 7,45835$, arrondi à 7 poissons

$N_8 = 7,62147$, arrondi à 8 poissons

$N_9 = 7,50844$, arrondi à 8 poissons

$N_{10} = 7,58804$, arrondi à 8 poissons

Le joueur 1 marque $6 + 7 + 7 + 7 + 8 = 35$ poissons

Le joueur 2 marque $8 + 8 + 8 + 8 + 8 = 40$ poissons

COMMENT BROSSER LA BALLE COMME BECKHAM OU L'ENVELOPPER COMME CARLOS

David Beckham et Roberto Carlos ont tiré quelques coups francs magistraux durant leur carrière de footballeur. Ces tirs semblent défier les lois de la physique. Peut-être que le plus stupéfiant fut celui du Brésilien Carlos contre la France en 1997. C'était un coup franc à 30 mètres. La plupart des footballeurs auraient fait une passe au lieu de tirer. Pas Roberto Carlos : il posa le ballon au sol et prit un élan de quelques pas.

Le gardien français, Fabien Barthez, aligna son mur défensif sans vraiment croire que Carlos allait viser sa cage. D'ailleurs, quand Carlos frappa, le ballon sembla se diriger bien loin de la cible. Les spectateurs d'un côté du but baissèrent la tête,

s'attendant à voir le ballon atterrir dans la foule. Mais soudain, au dernier moment, le ballon vira à gauche et pénétra dans le but derrière le gardien français. Barthez n'en croyait pas ses yeux. Il n'avait pas bougé d'un pouce. « Comment diable a-t-il fait cela ? » se demanda-t-il.

Le tir de Carlos ne défiait en rien les lois de la physique, mais illustrait la science, ou la technique, du toucher de balle. L'effet donné à un ballon de foot peut produire une trajectoire un peu folle. Si vous frappez franchement sans donner aucun effet, le ballon se déplace comme sur une feuille de papier à deux dimensions en traçant une parabole. Mais si vous y mettez de l'effet, les mathématiques de son déplacement deviennent tridimensionnelles. Au déplacement vers le haut et le bas s'ajoute l'inflexion vers la gauche ou la droite.

Mais qu'est-ce qui oriente le ballon vers la gauche ou vers la droite pendant sa course ? C'est l'effet Magnus, du nom du mathématicien Heinrich Magnus, qui, en 1852, fut le premier à expliquer l'effet de rotation d'un ballon. (Les Allemands vainqueurs de la Coupe du monde 2014 ont toujours été bons en football.) Le phénomène est semblable à ce qui crée la poussée sur l'aile d'un avion. Comme je l'ai expliqué page 355, les vitesses différentes de l'écoulement d'air au-dessus et au-dessous de l'aile diminuent la pression au-dessus de l'aile et l'augmentent au-dessous, produisant une force ascendante sur l'aile ; on parle de portance.

Pour voir la séquence du coup franc de Roberto Carlos, allez à <https://www.youtube.com/watch?v=1fKxsZP0TZg>

Pour que le ballon dévie vers la gauche, Carlos l'a frappé de telle sorte que son côté gauche tourne vers lui (autour d'un axe vertical passant par le centre du ballon). Cette rotation a eu pour effet de pousser l'air plus rapidement du côté gauche, ce qui a diminué la pression : le même effet que sur le haut d'une aile d'avion. La pression sur le côté droit du ballon augmente parce que la vitesse de l'air y décroît tandis que la surface du ballon est entraînée en rotation dans la trajectoire de l'écoulement d'air en cet endroit. La pression croissante se convertit en une force qui pousse le ballon de la droite vers la gauche... jusqu'au fond des filets.

C'est le même principe qui entraîne une balle de golf plus loin que les équations de Galilée le prévoient. Ici, l'axe de rotation est horizontal et perpendiculaire au déplacement de la balle. Quand la balle est éjectée du tee, la tête du club lui imprime une rotation telle que le bas de la balle tourne en direction du déplacement. Cela réduit la vitesse du courant d'air et, par l'effet Bernoulli, accroît la pression sous la balle, créant ainsi une force ascendante, ou portance, qui contrecarre la gravité. En fait, la balle ne pèse pratiquement rien durant son déplacement, comme si la rotation était une main qui la soutenait pour franchir la distance.

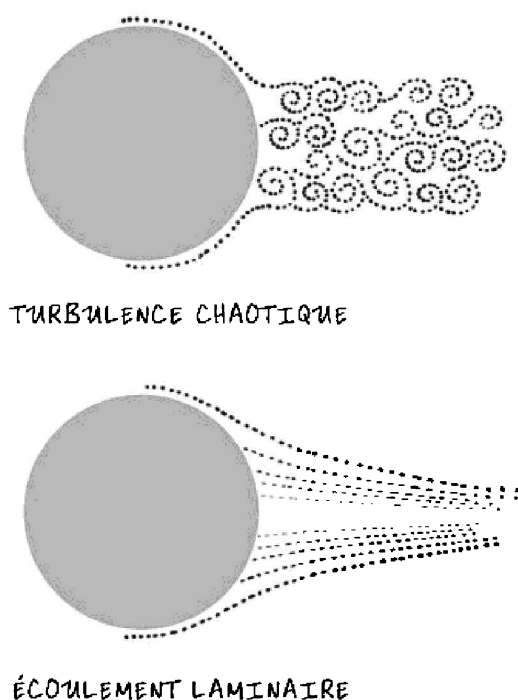


Fig. 5.13 La turbulence chaotique provoque moins de traînée que l'écoulement « laminaire » ordinaire.

Il y a un autre ingrédient que nous n'avons pas inclus et qui explique pourquoi le coup franc de Carlos s'est infléchi vers la gauche si tard : l'effet de la traînée sur le ballon. À l'instar de l'évolution en dents de scie de la population de lemmings, le secret derrière la magie du Brésilien est en fait un changement de comportement : de chaotique, il est devenu ordinaire. L'écoulement d'air derrière un ballon de football peut être chaotique ou ordinaire. L'écoulement chaotique, également appelé turbulent, se

produit quand le ballon se déplace très vite. L'écoulement ordinaire, ou laminaire, a lieu à des vitesses moindres. Le point de basculement de l'un à l'autre dépend du type de ballon.

Il est très facile de voir les différents écoulements d'air provoqués par différentes vitesses du vent. Marchez droit en tenant un drapeau (ou une bande de tissu) et regardez-le flotter dans votre sillage. Puis faites la même chose à plus grande vitesse, soit en tenant le drapeau à l'extérieur d'une vitre de voiture, soit en courant le plus vite possible face à un fort vent. Il va battre et claquer vivement. Tout simplement parce que l'air qui entoure un objet tel qu'un drapeau se comporte différemment selon la vitesse. À faible vitesse, l'écoulement d'air est facilement prévisible, mais à plus grande vitesse il est bien plus chaotique.

Quel effet ce changement d'écoulement turbulent en écoulement laminaire a-t-il sur la frappe d'un coup franc ? Il s'avère que la turbulence chaotique exerce beaucoup moins de traînée sur le ballon. Et donc, quand le ballon va vite, la rotation n'influence pas beaucoup sa direction, et la force de la rotation est répartie sur une plus grande distance de trajectoire. Quand le ballon ralentit et franchit le point de transition, la turbulence cède le pas à l'écoulement laminaire, lequel exerce une poussée bien plus forte, comme quelqu'un écrasant brutalement la pédale de frein. À cet instant de la transition, la résistance de l'air augmente de 150 %. La rotation exerce alors tout son effet et le ballon fait soudain un écart plus marqué. La traînée supplémentaire augmente aussi la portance, ce qui accentue l'effet Magnus et pousse le ballon encore plus fort vers le côté.

Il fallait à Roberto Carlos un coup franc suffisamment loin du but afin de pouvoir le frapper assez fort pour obtenir la turbulence chaotique et laisser au ballon le temps de ralentir et de virer avant de sortir du champ. Quand le ballon est frappé à environ 110 km/h, l'écoulement d'air qui l'entoure est chaotique, mais à environ mi-distance, quand il ralentit, la turbulence est modifiée. Les freins sont actionnés, la rotation de la balle prend le dessus et... l'infortuné Barthez est battu.

Ces principes mathématiques ne s'appliquent pas qu'au football. Le chaos affecte aussi nos voyages, particulièrement aériens. Pour la plupart d'entre nous, le mot « turbulence » évoque une invitation à attacher nos ceintures et le désagrément d'être secoués par des courants d'air chaotiques. Les avions sont bien plus rapides qu'un ballon de football, et l'écoulement chaotique, ou turbulent, sur leurs ailes augmente la résistance de l'air au déplacement de

l'avion, ce qui engendre une consommation accrue de carburant, donc un surcoût.

D'après une étude, une diminution de 10 % de la traînée turbulente pourrait augmenter de 40 % la marge bénéficiaire d'une compagnie aérienne. Les ingénieurs en aéronautique recherchent sans cesse des moyens d'améliorer la texture de la surface des ailes afin de rendre l'écoulement d'air moins chaotique. Une proposition consiste à introduire une rangée de rainures parallèles le long de l'aile, aussi rapprochées que les pistes d'un disque vinyle. Une autre serait de couvrir la surface de l'aile de minuscules structures en forme de dents, appelées denticules. D'ailleurs, la peau d'un requin est recouverte de denticules naturels, ce qui montre que la nature a découvert, bien avant les ingénieurs, comment vaincre la résistance des fluides.

Bien qu'elle ait fait l'objet de très nombreuses études, la turbulence derrière un ballon de football ou sous l'aile d'un avion demeure l'un des grands mystères des mathématiques. Il y a quand même une bonne nouvelle : nous savons désormais écrire les équations qui décrivent le comportement de l'air ou d'un fluide. La mauvaise nouvelle, c'est que personne ne sait comment les résoudre ! Ces équations ne sont pas importantes seulement pour Beckham ou Carlos. D'autres professions en ont besoin : les météorologues, pour prévoir les flux d'air dans l'atmosphère ; les médecins, pour comprendre la circulation du sang dans le corps ; et les astrophysiciens, pour déterminer le déplacement des étoiles dans les galaxies. Tous ces phénomènes sont régis par les mêmes équations mathématiques. Pour l'instant, que ce soient les prévisionnistes ou les concepteurs, tous doivent se satisfaire d'approximations, et, parce que le chaos se cache derrière ces équations, une petite erreur peut signifier de grandes conséquences sur le résultat. Les prévisions peuvent ainsi se révéler complètement fausses.

Ces équations sont appelées équations de Navier-Stokes, d'après les deux mathématiciens du XIX^e siècle qui les ont formulées. Elles ne sont pas simples, comme en témoigne l'une de leurs représentations courantes :

$$\frac{\partial}{\partial t} u_i + \sum_{j=1}^n u_j \frac{\partial u_i}{\partial x_j} = v \quad u - \frac{\partial p}{\partial x_i} + f_i(x, t)$$

$$\operatorname{div} u = \sum_{i=1}^n \frac{\partial u_i}{\partial x_i} = 0$$

Si vous ne comprenez pas certains des symboles dans ces équations, dites-vous bien que vous n'êtes pas le seul ! Mais pour ceux qui connaissent le langage des maths, elles contiennent la clé pour prévoir le futur. Elles sont si importantes qu'un prix d'un million de dollars est offert à la première personne qui les résoudra.

Le grand physicien allemand Werner Heisenberg, l'un des fondateurs de la physique quantique, a dit :

Lorsque je rencontrerai Dieu, je lui poserai deux questions : pourquoi la relativité ? Et pourquoi la turbulence ? Je suis personnellement convaincu qu'il aura une réponse à la première.

Quand on demanda à Roberto Carlos comment il était parvenu à imprimer au ballon une trajectoire aussi courbe, il répondit :

Dès mon plus jeune âge, je me suis entraîné à la précision des coups francs. J'avais l'habitude de rester une heure après chaque séance d'entraînement pour m'exercer. C'est comme pour tout : plus vous souffrez et transpirez, plus vous obtenez des résultats !

Ça doit être vrai aussi des mathématiques. Plus le problème est difficile, plus sa résolution est gratifiante. Aussi, si le travail mathématique devient ardu, souvenez-vous des mots de Roberto Carlos : « Plus vous souffrez et transpirez, plus vous obtenez des résultats ! » Et quand, finalement, vous résoudrez l'une des plus grandes énigmes mathématiques de tous les temps, tout le monde pensera comme Barthez voyant la balle au fond des filets : comment diable a-t-il fait ça ?

APPENDICES

Remerciements

Je me dois d'abord de remercier ceux qui m'ont aidé à concevoir ce livre : mon éditeur Robin Harvie à Fourth Estate, dont l'amour des supermarathons nous a très certainement été précieux ; mon agent Antony Topping chez Greene & Heaton, qui se comporte comme un véritable coach personnel à chacun de mes marathons littéraires ; mon relecteur John Woodruff, qui a renoncé à partir à la retraite pour pouvoir mettre en forme ce livre ; et mes deux illustrateurs : Joe McClaren, dont les dessins pour mes chroniques du *Times* ont ensoleillé mes mercredis matin, et Raymond Turvey, qui a parfaitement saisi les formes même les plus complexes que je lui soumettais.

Le contenu de ce livre trouve sa source dans plusieurs projets.

La Royal Institution of Great Britain, une des plus anciennes sociétés savantes de Grande-Bretagne, m'a demandé de donner les Christmas Lectures en 2006. Ces conférences, qui se tiennent depuis 1825, sont retransmises à la télévision depuis 1966, à l'époque de Noël comme leur nom l'indique. Elles visent à populariser les sciences, et plus particulièrement à inciter les plus jeunes à *faire* science. J'ai eu la chance d'assister, en 1978, à la première de ces conférences consacrée aux mathématiques — elle était donnée par Christopher Zeeman. J'avais treize ans. Zeeman a abordé un ensemble tellement passionnant de sujets que je suis sorti de là sachant exactement ce que je voulais devenir : mathématicien, comme lui. Me demander à mon tour de donner ces conférences fut pour moi une merveilleuse occasion de remercier la Royal Institution de m'avoir inspiré cette vocation. Pouvoir passionner une nouvelle génération de mathématiciens est un réel honneur.

Mon cahier des charges consistait à produire cinq conférences destinées aux onze-quatorze ans. Les Christmas Lectures parlent d'explosions et de glace sèche et font participer des membres du public aux expériences. Trouver des choses à faire exploser pour le plaisir et imaginer des jeux amusants pour illustrer les maths s'est avéré un défi des plus stimulants. J'ai eu l'impression de donner cinq one-man-show. Pour créer ces conférences, j'avais autour de moi la formidable équipe de la Royal Institution, Channel Five et Windfall Films, la société chargée de la production télévisée. J'aimerais particulièrement remercier Martin Gorst, Tim Edwards et Alice Jones, qui m'ont aidé à trouver les moyens de rendre les mathématiques aussi vivantes. J'aimerais aussi remercier Andy Marmery, Catherine de Lange, David Dugan et David Coleman, sans qui ces conférences n'auraient pas pu avoir lieu.

Nous avons testé ce contenu dans de nombreuses écoles, mais j'aimerais en particulier remercier la Jewish Free School, qui s'est montrée très tolérante en permettant à ses élèves d'être exposés à un large éventail d'idées. Noël et le judaïsme ne vont pas nécessairement de pair, mais je crois que nous sommes

parvenus à montrer que les mathématiques sont avant tout un langage universel. En observant les réactions des enfants, nous avons pu voir ce qui fonctionnait ou non. L'ensemble des recherches menées pour ces conférences nous ont été très utiles pour décider du contenu de ce livre.

En me permettant de découvrir quels aspects des mathématiques pouvaient intéresser un public plus large, la réalisation de programmes télévisés m'a été très précieuse. Je voudrais remercier Alom Shaha, avec qui j'ai fait quatre épisodes de l'émission intitulée *Painting with Numbers* pour Teachers TV, ainsi qu'un film sur la preuve apportée par Euclide qu'il y a une infinité de nombres premiers, et auquel participa mon équipe de foot, le Recreativo Hackney. Les contenus abordés dans ces émissions ont également beaucoup contribué aux Christmas Lectures.

The Story of Maths, la série en quatre parties que j'ai réalisée avec la BBC, a fourni une formidable base historique à nombre d'anecdotes dans ce livre. J'aimerais remercier mon producteur exécutif à la BBC, David Okuefuna, dont l'amour des maths fut à l'origine de l'idée de la série. The Open University a apporté un précieux soutien financier et académique. Lorsque le tournage commence, ces émissions deviennent un réel travail d'équipe, et je voudrais particulièrement remercier Karen McGann, Krysia Derecki, Robin Dashwood, Christina Lowry, David Berry et Kemi Majekodunmi.

Écrire des livres, réaliser des séries télévisées et présenter des conférences pour donner vie aux mathématiques demande beaucoup de temps. Je suis reconnaissant à ceux qui m'ont permis d'en disposer. Charles Simonyi a compris le premier qu'une chaire de vulgarisation scientifique offrait un formidable espace à son titulaire pour fasciner le public avec les sciences. L'université d'Oxford a toujours soutenu mes efforts pour porter les maths au grand public. J'ai également bénéficié d'un précieux soutien de la part de l'Engineering and Physical Sciences Research Council dans le cadre de leur formidable programme Senior Media Fellowship. Sans tous ces soutiens, je n'aurais jamais pu être aussi efficace.

Je voudrais aussi remercier les Mathemagicians, une troupe d'étudiants de l'université d'Oxford qui m'aide, par des moyens très divers, à diffuser la joie des maths. Beaucoup de ces étudiants ont lu les premières versions de ce livre et ont eu la stimulante idée d'une application pour l'accompagner. Thomas Woolley m'a tout particulièrement aidé en créant certaines des fractales complexes présentées ici.

Ceux qui ont lu ce livre auront, je pense, perçu mon goût pour le foot. Jouer pour mon équipe de la Sunday League, le Recreativo Hackney (voir <http://recreativofootballclub.blogspot.com>), m'a permis, chaque dimanche, de décompresser (même si une fracture du cinquième métacarpe de la main droite et une opération chirurgicale après fracture du poignet gauche dues à des accidents footballistiques ont quelque peu retardé la publication de ce livre). Je suis supporter d'Arsenal. Et même s'ils n'ont remporté aucun trophée depuis quelque temps, quand je les regarde jouer, j'ai à chaque fois l'impression d'assister à une partie complexe d'échecs. Je mettrais ma main à couper qu'ils ont un mathématicien sur le banc. Et pour finir, grâce aux livres que j'ai écrits, j'ai eu droit à un bonus footballistique inattendu : une convocation pour jouer au sein de la England Writers Football Team (voir <http://writersteam.co.uk>) !

Tous les écrivains de cette équipe s'accorderont à dire que c'est à notre

famille que nous devons le plus, pour son soutien sans faille dans cette épreuve que constitue l'écriture d'un livre. À ma femme Shani et mes trois enfants Tomer, Magaly et Ina : merci. Mon chat, Freddie Ljungberg, n'a malheureusement pas supporté la pression et a quitté le foyer. La dernière fois qu'on l'a aperçu, je crois c'était du côté de West Ham.

Les Éditions Héloïse d'Ormesson remercient Jean-Michel Kantor pour son expertise mathématique et sa relecture vigilante.

Crédits des illustrations

CHAPITRE PREMIER

- 1.01 Joueurs de foot portant des nombres premiers © Joe McLaren
- 1.02 Cigales ayant un cycle de vie de 7 ans © Joe McLaren
- 1.03 Cigales ayant un cycle de vie de 9 ans © Joe McLaren
- 1.04 Partition du *Quatuor pour la fin du temps* de Messiaen © Éditions Durand, Paris. Reproduit avec l'autorisation de G. Ricordi & Co (Londres) Ltd, département d'Universal Music Publishing Group
- 1.05 Message d'Arecibo — reproduit avec l'aimable autorisation de la NASA
- 1.06 Le nombre 200,201 écrit en hiéroglyphes © Joe McLaren
- 1.07 Symboles égyptiens pour les puissances de 10 © Joe McLaren
- 1.08 Le nombre 71 en cunéiforme © Joe McLaren
- 1.09 Symbole du nombre 10 © Joe McLaren
- 1.10 Décompte de haricots © Raymond Turvey
- 1.11 Le nombre 3 607 en cunéiforme © Joe McLaren
- 1.12 Mains pour compter © Raymond Turvey
- 1.13 Le nombre 17 chez les Mayas © Joe McLaren
- 1.14 Le nombre 13 en hébreu © Joe McLaren
- 1.15 Le nombre 23 en caractères chinois © Joe McLaren
- 1.16 Bâtons de bambou © Raymond Turvey
- 1.17 Bâtons de bambou © Raymond Turvey
- 1.18 Crible © Raymond Turvey
- 1.19 Crible © Raymond Turvey
- 1.20 Crible © Raymond Turvey
- 1.21 Marelle des nombres premiers © Joe McLaren
- 1.22 Lapins © Joe McLaren
- 1.23 Spirale de Fibonacci © Joe McLaren
- 1.24 Échiquier avec riz © Joe McLaren
- 1.25 Dés de nombre premier © Joe McLaren

CHAPITRE II

- 2.01 La tour de Watts © Joe McLaren
- 2.02 Sphère tranchée © Raymond Turvey
- 2.03 Ballons de football © Joe McLaren
- 2.04 Les solides de Platon © Joe McLaren

- 2.05 Tétraèdre tronqué © Raymond Turvey
- 2.06 Grand rhombicosidodécaèdre convexe © Raymond Turvey
- 2.07 Ballons de foot © Raymond Turvey
- 2.08 Ballon de foot © Raymond Turvey
- 2.09 Deux bulles fusionnées © Joe McLaren
- 2.10 Bulles fusionnées en forme de cacahuète © Joe McLaren
- 2.11 Bulles fusionnées © Joe McLaren
- 2.12 Bulles fusionnées © Joe McLaren
- 2.13 Armature en fil de fer © Joe McLaren
- 2.14 Tétraèdre © Joe McLaren
- 2.15 Octaèdre tronqué © Raymond Turvey
- 2.16 Mousse de Kelvin © Raymond Turvey
- 2.17 Formes de Weaire et Phelan © Raymond Turvey
- 2.18 Centre olympique de natation de Pékin © Arup
- 2.19 Dodécaèdre rhombique © Raymond Turvey
- 2.20 Maquette balles de ping-pong et baguettes © Raymond Turvey
- 2.21 Trois cartes de la Grande-Bretagne © Joe McLaren
- 2.22 Réaliser une fractale © Raymond Turvey
- 2.23 Réaliser une fractale © Raymond Turvey
- 2.24 Réaliser une fractale © Raymond Turvey
- 2.25 Littoral (fractale) © Thomas Woolley
- 2.26 Flocon de Koch
- 2.27 Littoral (fractale) © Thomas Woolley
- 2.28 Littoral (fractale) © Thomas Woolley
- 2.29 Littoral écossais selon trois degrés de grossissement © Steve Boggs
- 2.30 Fougère fractale
- 2.31 Quatre fractales sur papier millimétré © Thomas Woolley
- 2.32 Six fractales © Thomas Woolley
- 2.33 Cinq cartes de la Grande-Bretagne © Thomas Woolley
- 2.34 Dimensions fractales d'une peinture © Joe McLaren
- 2.35 Puzzle de Descartes © Raymond Turvey
- 2.36 Grande Arche de la Défense, Paris © Getty images
- 2.37 Cube quadridimensionnel © Joe McLaren
- 2.38 Plan géométrique du métro de Londres
- 2.39 Sphère, tores © Raymond Turvey
- 2.40 Anneaux entrelacés © Raymond Turvey
- 2.41 Sphère © Raymond Turvey
- 2.42 Tore © Raymond Turvey
- 2.43 Carte de l'Europe
- 2.44 Sept couleurs © Joe McLaren
- 2.45 Délier deux anneaux entrelacés © Raymond Turvey

CHAPITRE III

- 3.01 Lézards © Joe McLaren
- 3.02 Grille de loterie © Raymond Turvey
- 3.03 Grille gagnante © Raymond Turvey

- 3.04 Dés tétraédriques © Raymond Turvey
- 3.05 Dés © Raymond Turvey
- 3.06 Icosaèdre © Raymond Turvey
- 3.07 Pentakidodécaèdre © Raymond Turvey
- 3.08 Pyramide de dés © Raymond Turvey
- 3.09 Roulette chocolat-piment © Joe McLaren
- 3.10 Roulette chocolat-piment agencée © Joe McLaren
- 3.11 Plats et parts de gâteau © Raymond Turvey
- 3.12 Le carré magique de Dürer © Joe McLaren
- 3.13 Carte simplifiée des ponts © Raymond Turvey
- 3.14 Enveloppe © Raymond Turvey
- 3.15 Carte du XVIII^e siècle © Joe McLaren
- 3.16 Carte du XXI^e siècle © Joe McLaren
- 3.17 Problème du représentant de commerce © Raymond Turvey
- 3.18 Problème des invités © Raymond Turvey
- 3.19 Frontières © Raymond Turvey
- 3.20 Champ de mines © Raymond Turvey
- 3.21 Champ de mines © Raymond Turvey
- 3.22 Problème du chargement d'un camion © Joe McLaren
- 3.23 Solution au problème du représentant de commerce © Raymond Turvey

CHAPITRE IV

- 4.01 Code Babington © Joe McLaren
- 4.02 Machine Enigma © Joe McLaren
- 4.03 Système des frères Chappe © Joe McLaren
- 4.04 Code des frères Chappe © Joe McLaren
- 4.05 Sémaphore de Nelson © Raymond Turvey
- 4.06 L'alphabet sémaphore © Joe McLaren
- 4.07 Couverture de l'album des Beatles © Joe McLaren
- 4.08 Couverture de l'album des Beatles corrigée © Joe McLaren
- 4.09 Symbole du CDN
- 4.10 Code Morse © Raymond Turvey
- 4.11 « Morse » en code Morse © Raymond Turvey
- 4.12 Hexagramme © Raymond Turvey
- 4.13 Hexagramme © Raymond Turvey
- 4.14 Photographie du calculateur binaire de Leibniz © Marcus du Sautoy
- 4.15 Couverture de l'album de Coldplay © Raymond Turvey
- 4.16 Code Baudot © Raymond Turvey
- 4.17 Horloges © Raymond Turvey
- 4.18 Courbe elliptique © Steve Boggs
- 4.19 Courbe elliptique © Steve Boggs

CHAPITRE V

- 5.01 Plan éclipse © Joe McLaren
- 5.02 Équation dessinée à la main © Marcus du Sautoy
- 5.03 Diagramme des forces agissant sur un boomerang © Raymond Turvey
- 5.04 Boomerang © Raymond Turvey
- 5.05 Orbites elliptiques © Raymond Turvey
- 5.06 Pendule © Raymond Turvey
- 5.07 Champ magnétique © Joe McLaren
- 5.08 Lemming © Joe McLaren
- 5.09 Graphique population de lemmings © Raymond Turvey
- 5.10 Graphique population de lemmings © Raymond Turvey
- 5.11 Graphique population de lemmings © Raymond Turvey
- 5.12 Graphique population de lemmings © Raymond Turvey
- 5.13 Turbulence chaotique et écoulement laminaire © Joe McLaren

Index

Abbassides, dynastie des 265
Acide désoxyribonucléique (ADN) 38, 164, 259
Afrique du Sud 147, 180
Alexandrie 58
ALFRED, roi des Anglo-Saxons, dit le Grand 193
Algèbre 333, 351-353
Algorithme 58, 352
AL-KHWARIZMI, Muhammad ibn-Musa 352-353
AL-KINDI, Yaqub 265
Allemagne 93, 101, 107, 170, 272, 388
Amas globulaire M 13 38-39
Amérique 25, 27, 30, 181, 183, 342
Analyse fréquentielle 265, 267, 269-272, 274-275, 277-278, 285
Angleterre 19, 102, 109, 197, 281-282
 Voir Grande-Bretagne 19
Apollo 15 344
Arabes 231, 265
ARCHIMÈDE 98-100, 105-108, 111, 117, 123-124, 129, 213-214, 216
Arctique 373, 378
Arecibo 38-39
ARISTAGORAS 260
ARISTOTE 344
Arup 117, 126-127
Asie 88
Asteroids (jeu) 161, 165, 171, 173-174
AUGUSTIN D'HIPPONE (*La Cité de Dieu*) 52
Australie 147

BABBAGE, Charles 271
BABINGTON, Anthony 268
Babyloniens 41-42, 44-48, 55, 209, 349-352
Backgammon 210
Bagdad 352
Ballon de football 100-108, 213, 387-395
 Voir Football 100
Baltique 238
Barcelone 232
BARTHEZ, Fabien 387-388, 392, 395

BAUDOT, Émile 289, 292-295, 304
 Beatles (*Help*) 283-284
 BECK, Harry 163
 BECKHAM, David 19-20, 23, 32, 347-348, 353, 387, 393
 BEETHOVEN, Ludwig van (*Cinquième Symphonie*) 284-285, 288
 Belgique 170
 BERG, Alban 32-33
 BERNOULLI, Daniel 355, 389
 Big Bang 172-173, 264
 BIRCH, Bryan 333
 Bletchley Park 277
 Boomerang 354-360, 376
 Bristol 97
 BROWN, Dan (*Da Vinci Code*) 75
 Bulle 96-100, 117-127

Calendrier 48-49, 52, 103, 338-340
 Californie 84-85, 180, 374
 CALVINO, Italo 235
 Cambridge 37, 277
 CARLOS, Roberto 387-390, 392-395
 Carré gréco-latin 235-237, 239
 Carré magique 228, 230-233, 235-237, 239
 Carte à puce 333
 Casino 203-206, 208, 376-377
 CASPAR, Donald 115
 CATALAN, Eugène 129
 Celtes 181
 CÉZANNE, Paul 185
 CHANG, Hun-yu 88
 Chaos 20, 151, 363, 366-369, 371, 374, 377-378, 383-384, 387, 390-393
 CHAPPE, Claude et Ignace 279-281
 Chicago Bulls 19
 Chiffre de substitution 262-265, 267-268, 270-272, 274-275, 277-278
 Chinois 25, 53-55, 66, 180, 260, 278
 Choix aléatoire 184-185, 194
 Cigale 25-30, 35
 CLAY, Landon 12
 Cochin (Inde) 211
 Code binaire 36, 38, 225-226, 289-295
 Code informatique 305, 307, 310-314, 324, 326-327
 Code visuel 278-279, 282, 284-285
 Coldplay 289, 293-295, 304
 COLOMB, Christophe 340, 342-343
 COLOMB, Ferdinand 343
 Condé-sur-L'Escaut 281
 COOPER, Bob « The Rock » 183
 Coran 352

CRICK, Francis 115
 Cristallographie aux rayons X 130
 Cryptage par courbe elliptique (Elliptic Curve Cryptography, ECC) 328-329, 331-333
 Cryptanalyse 265, 267, 269-271, 274-275, 277-278
 Cube 158-160
Cube (film) 34-35
 Cube d'eau (piscine olympique de Pékin) 116, 125-126

DALÍ, Salvador (*Crucifixion, Corpus Hypercubus*) 159-160
 DARIUS I^{er} DE PERSE 260
 DAVIS, Miles 14
 Dé 92-94, 208-217
 Démineur (jeu) 253
 DESCARTES, René 81, 152-154, 157
 DIACONIS, Persi 374-375
 Dodécaèdre 103-104, 124, 128, 175-176, 215
 Donjons et Dragons 211-212
 Dublin 124
 DÜRER, Albrecht (*Melencolia*) 232
 DYLAN, Robert Zimmerman, dit Bob (*Day of the Locusts*) 26

Échiquier 79-80
 Éclipse 337, 341-342
 Écosse 140, 268, 307
 Voir Grande-Bretagne 140
 EDWARDS, Ken 238
 Effet gyroscopique 355-356, 376
 « Effet papillon » 372
 Égyptiens 25, 40-42, 47, 55, 181, 209
 ÉLISABETH I^{re} 82, 268-269
 ELVERICH, Hans-Michael 84
 Enigma 272-277
 Équation du second degré 45
 Équation quadratique 349-351, 353
 ÉRATOSTHÈNE 59-60, 63
 ERDÖS, Paul 67
 Espagne 133
 États-Unis 19, 27, 83, 98, 161, 204, 212
 EUCLIDE 60-62, 64-65, 104
 EULER, Leonhard 82, 234, 236, 239-241, 245-246, 319, 323, 327
 Euphrate 42, 349
 Europe 81, 170-171, 232, 252, 269, 278, 342-343, 371, 374
 Extraterrestres 18, 36
 Extrême-Orient 181

FERMAT, Pierre de 66-67, 81, 201, 308, 316, 318-319, 321-322, 327
 FIBONACCI, Leonardo 73-79, 186-187

FINER, Jem (Jeremy Max) 33
 FINKEL, Irving 210
 FLAUBERT, Gustave 235
 Flocon de neige 95, 127, 130-131
 Fonction zêta 94
 Football 19, 23, 100-102, 105, 107-108, 246-247, 347, 374, 388
 Voir Ballon de football 19
 Fougère 141-142
 Fractales 132, 136, 141-143, 145, 147, 149-151, 369
 France 170, 275, 281, 373, 379, 387
 FREEMAN, Robert 283
 FRÉNICLE DE BESSY, Bernard 233
 FURMAN, Ashrita 238

GALILÉE (Gahileo Galilei) 95, 344-347, 360-362, 364, 389
 GARLAND, Alex (*Tesseract*) 160
 GAUDÍ, Antonio 232
 Gaule 262
 GAUSS, Carl Friedrich 91-93, 202, 285
 Gematria 49
 Géométrie 95-96, 106, 108, 141, 153-154, 161-163, 173-174, 214, 245, 330, 332, 355, 369
 Google 245
 Görlitz 30
 Göttingen 93, 285
 Grande Arche (Paris) 156-158
 Grande-Bretagne 98, 132-133, 137, 139, 147
 Voir Angleterre, Écosse 132
 Gravité 344, 346-347, 360
 Great Internet Mersenne Prime Search (GIMPS) 83-85
 Grèce, Grecs 25, 55-56, 59, 81, 162, 172, 329-330
 Greenwich 153
 Grenade 127-129
 Grippe espagnole 113
 Guatemala, Guatémaltèques 47, 49
 Guinness des records 237-241, 243, 245

HADAMARD, Jacques 92
 HADDON, Mark (*Le Bizarre Incident du chien pendant la nuit*) 34
 HARDY, Godfrey Harold (*L'Apologie d'un mathématicien*) 37, 268
 Harvard 139
 HAZEL, Martin 238
 Hébreux 49, 51, 55
 HEISENBERG, Werner 394
 HERGÉ, Georges Remi, dit (*Le Temple du Soleil*) 337, 340
 Hexagone 105-107, 111, 117, 122-124, 128-129, 131, 143, 178, 213-214
 Hexaki-icosaèdre 216
 HISTIÉE 260

HOLMES, Susan 375
HOOKE, Robert 278-279
Horloge modulaire 66, 314-317, 319, 321-322, 324-327
HURWITZ, Alex 85
Hypercube 158, 160

Icosaèdre 103-105, 113, 115-116, 212, 215
Icosidodécaèdre tronqué 107
Incas 337
Inde 45, 77, 79, 211, 231
Indiens d'Amérique 278
Induction 242
International Standard Book Number (ISBN) 295, 297-298
Internet 83, 307-311, 314, 322, 324, 326-327
Irak 42, 209, 351
Iran 42, 260
Islam 231, 352
Italie 188, 259, 374
iTunes 293

JAMES, Andi 238
Japon 180
JARVIS, Frazer 236
JÉSUS-CHRIST 160, 232
JOHNSON, Norman 129
Joint Photographic Experts Group (JPEG) 293
JORDAN, Michael 19
Judaïsme 49, 52
JULES CÉSAR 20, 262-263

Kabbale 49
Kamasutra 261-265
KELVIN, William Thomson, Lord 123-125
KEPLER, Johannes 127-129, 131
KLUG, Aaron 115
KOCH, Helge von 137, 142, 145
Königsberg (Kaliningrad) 238-240, 243-245

LA Galaxy 23
La Haye-Descartes 153
La Mecque 339, 352
Latitude et longitude 153
LA VALLÉE POUSSIN, Charles de 92
LEIBNIZ, Gottfried Wilhelm 99, 289-292
LEJEUNE DIRICHLET, Gustav 308
Lemming 378-384, 387, 390
LÉONARD DE VINCI 258

Lézard à flancs maculés (*Uta stansburiana*) 181-182
Lille 281
Londres 23, 33, 80, 111, 153, 163, 210, 239, 278, 377
Longplayer (installation) 33
Loterie 188-191, 193, 195, 197, 202, 257
Lune 59, 232, 338-345, 365
Luo (rivière) 230
Luxembourg 170

Madrid 23
Magie 161, 198
MAGNUS, Heinrich 388, 392
Manchester United 17, 19, 247
MANDELBROT, Benoît 139-141
Marelle 68-72
MARIE I^{re} D'ÉCOSSE (Marie Stuart) 268-269, 307
MARTIN, Apple Blythe Alison 64
MARTIN, Chris (Christopher) 64, 294
MARTINEZ, David 147
Mayas 47-49, 55
MERSENNE, Marin 52, 81-85, 87
MESSIAEN, Olivier (*Quatuor pour la fin du temps*) 30-33
Météorologie 336, 371-373, 377-378, 393
Métro (londonien) 163, 238, 245
Mexico 105
Mexique 47
Milet 260
MITTAG-LEFFLER, Gösta 366
MITTERRAND, François 156
Monopoly 217, 223
MONTGOMERY, Richard 375
Morse (code) 285, 288, 292
MORSE, Samuel 285
Mousse 117, 122-125, 127
MOZART, Wolfgang Amadeus 14
MUSSOLINI, Benito 189

National Aeronautics and Space Administration (NASA) 38, 305, 345
NAVIER, Henri 394
NELSON, Horatio 281-282, 307
NÉRON 50
NEWTON, Isaac 99, 172, 365, 367, 376
Nil 40, 59
Nim (jeu) 225-226, 289
Nombres parfaits 51-52
Norvège 147, 149

Octaèdre 103-104, 212, 216
 Orbite 365
 Oregon 147
 OSCAR II DE SUÈDE ET DE NORVÈGE 364
 Oxford 277
 OZANAM, Jacques 233

PALTROW, Gwyneth 64
 PAPPUS D'ALEXANDRIE 106
 Paris 156-157, 159, 281
 PASCO, John 282
 Pékin 116, 126
 Pendules 360-364, 367-369
 Pentagone 105, 124
 Pentakidodécaèdre 215
 PEREC, Georges (*La Vie mode d'emploi*) 235, 265
 PERELMAN, Grigori 176-177
 PHELAN, Robert 124-125
 PHELIPPES, Thomas 269
 PHRAGMEN, Lars 366
 Pierre-feuille-ciseaux 180-181, 183-185, 194
 Pile ou face 307-310, 374-375
 Pise 344-345, 361-362, 378
 PLANCK, Max 136
 PLATEAU, Joseph 120-123, 125-126
 PLATON 60, 96, 101-106, 111, 115, 128-129, 176, 212-213, 215
 PLUTARQUE 106
 Pagues 33
 POINCARÉ, Henri 164-165, 176, 364-367, 370, 376
 POINSOT, Louis 129
 Poker (*perfect shuffle*) 198-202
 POLLOCK, Jackson (*No. 5, 1948 ; Blue Poles*) 147, 149
 Pologne, Polonais 275, 277
 Polyèdre flexible 129
 POPHAM, Home Riggs 282
 PORTA, Giovanni 259
 Portugal 133
 Poumon (humain) 95, 141
 Pregel 238-239, 245
 Premier League 246-249
 Preston 102
 Princeton 26
 Problème NP-complet 249-255
 Puerto Rico 38
 PYTHAGORE 45

RAÛL (Raúl González Blanco) 19, 23
 Real Madrid 19, 21, 23-25

Recreativo Hackney 23
Rhombicosidodécaèdre convexe 107
RIEMANN, Bernhard 93-94, 202
ROBINSON, Raphael 85
Romains 108
RONALDO (Ronaldo Luis Nazário de Lima) 23
ROONEY, Wayne 347-348, 353-354
RUSSELL, Ed 236

SACKS, Oliver (*L'Homme qui prenait sa femme pour un chapeau*) 65
SAGAN, Carl (*Contact*) 36-37
Sagrada Familia (Barcelone) 232
Saint-Pétersbourg 239
Salvador 47
SANTELIA, Michele 237
SCHROEPPPEL, Richard 233
SCHWARZ, Hermann 100
Science-fiction 36-37
SCOTT, David 344
Scrabble 265
Scytale 260
Sémaphore 283
SHAKESPEARE, William 14
SHAO YONG 290
Signaux de fumée 278
SMITH, Edson 85-87
Soleil 26, 59, 120, 141, 175, 336-342, 345, 365, 370-371
Solides d'Archimède 98, 105-108, 111, 117, 123, 129, 213, 215
Solides de Johnson 129
Solides de Platon 96, 101, 103-106, 111, 115, 128, 130, 176, 212, 215
Solides de Poincaré 129
Spartiates 260
Sphère 96-101, 103, 117
SPRECKELSEN, Johan Otto von 156-157
Stéganographie 261
STEINBECK, John 14
STOKES, George Gabriel 394
Structure alvéolaire 123
Sudoku 233, 235-237, 254
Suède 364
SULLIVAN, Thomas 109
Suse 260
SWINNERTON-DYER, Peter 333
Syracuse 108
Syrie 42
Système solaire 364-365, 367, 369-371

Taipei 88

TARRY, Gaston 234
TAYLOR, Jean 122
TAYLOR, Richard 147, 150-151
Téléphonie 333, 377
Terre 26, 36, 38, 59, 104, 135, 162, 165, 167, 170, 173, 175, 336, 338-342,
344-345, 347, 365, 370-371
Tétraèdre 102, 128, 131, 209-210, 212
Tétrakaidécaèdre 124
Thé 109-113, 165
Tibétains 33
Tintin 337-338, 340
Topologie 163-165, 245
Touraine 153
Trafalgar (bataille) 282
Triangle 45, 102-103, 215-216
Tube Challenge 238, 245
Turbulence 336, 390-394
Turquie 260

Université de Californie à Los Angeles (UCLA) 85
Upsilon Andromedae 369
Ur 209-211

VAN GOGH, Vincent 185
Venise 188
Vienne 278
VIGENÈRE, Blaise de 271-272
VIRAHANKA 77
Virus 114-116
Voyager 2 305

WACKHER, Matthäus 130
WATSON, James 115
WATTS, William 97-98
WEAIRE, Denis 124-125
WEBER, Wilhelm 285
WILSON, Steve 238
WOOLLEY, sir Leonard 209

Yi Ching. Le Livre des changements 289
YU (empereur de Chine) 230

ZAPPA, Diva Thin Muffin Pigeon 64
ZAPPA, Frank 64
ZAPPA, Moon Unit 64
Zéro 44-45, 48
ZIDANE, Zinedine 23

Titre original :
THE NUMBER MYSTERIES.
A MATHEMATICAL ODYSSEY THROUGH
EVERYDAY LIFE

Éditeur original : Fourth Estate
© Marcus du Sautoy, 2010.
© Éditions Héloïse d'Ormesson, 2014,
pour la traduction française.

Couverture : Illustration Aude Van Ryn.

Éditions Gallimard
5 rue Gaston-Gallimard
75328 Paris
<http://www.gallimard.fr>

DU MÊME AUTEUR

LA SYMÉTRIE OU LES MATHS AU CLAIR DE LUNE, Éditions Héloïse d'Ormesson, 2012 ; Points, 2013.

LA SYMPHONIE DES NOMBRES PREMIERS, Éditions Héloïse d'Ormesson, 2005 ; Éditions du Seuil, coll. Points, 2007.

Marcus du Sautoy

Le mystère des nombres

Odyssée mathématique à travers notre quotidien

Traduit de l'anglais par Hélène Borraz

Nul ne peut plus ignorer combien les mathématiques sont fondamentales et omniprésentes dans notre quotidien. Mais mesure-t-on réellement à quel point ?

Sait-on par exemple que Wayne Rooney, l'attaquant de Manchester United, résout une équation quadratique chaque fois qu'il récupère un centre pour marquer un but ?

Que nous utilisons les nombres premiers lorsque nous passons une commande sur Internet ?

Ou encore que l'on peut gagner un million de dollars rien qu'en résolvant une énigme du *Mystère des nombres* ?

Marcus du Sautoy est footballeur, musicien amateur, vulgarisateur de génie et professeur de mathématiques à l'université d'Oxford. Il révèle la beauté qui se cache derrière les mathématiques, ce langage qui nous permet de déchiffrer l'univers et de développer les technologies actuelles.

Le profane ne sera pas le dernier à succomber à cette science rendue lumineuse.

Cette édition électronique du livre
Le mystère des nombres de Marcus du Sautoy
a été réalisée le 31 août 2015 par les Éditions Gallimard.
Elle repose sur l'édition papier du même ouvrage
(ISBN : 9782070465880 - Numéro d'édition : 287126).
Code Sodis : N75110 - ISBN : 9782072621895.
Numéro d'édition : 287128.

Ce document numérique a été réalisé par Nord Compo