Préambule

Nul ne peut exactement prédire l'évolution de la situation dans les jours prochains, entre un mouvement puissant et un pouvoir habile à manœuvrer. En attendant une reprise des cours, je vous propose la rédaction, un peu élargie, des trois premières semaines de cours et une rédaction de chapitres qui constitueront la suite du cours, à quelques variantes près, minimes sans doute, dont je pourrai avoir l'idée.). Il va de soi qu'il s'agit, pour ces derniers chapitres, de notes qui ne remplacent en aucune façon le cours oral où ces sujets seront présentés et discutés.

Pour toute question, me contacter ; mon adresse électronique est :

jean-pierre.escofier@univ-rennes1.fr

Table des matières

Chapitre 1

Mathématiques financières

1.1 Introduction

Si je me considère comme un amateur (et non un chercheur professionnel) en histoire des mathématiques, je dois encore plus le souligner en abordant un chapitre consacré aux mathématiques financières comme premier des chapitres de mon cours du second semestre de cette année 2008-2009 de L3 de mathématiques. Mais il me semble impossible qu'on ne parle pas, dans un enseignement de mathématiques à l'université, des liens entre les mathématiques et le monde financier alors qu'une crise d'une ampleur exceptionnelle vient de frapper l'ensemble des systèmes financiers de la planète et que le rôle qu'y aurait joué les mathématiques a été l'objet d'opinions très critiques parfois. Et même si je n'y connais pas grand chose, je vais en dire quelques mots, en mettant en garde mes auditeurs et auditrices, mes lectrices et lecteurs : gardez votre sens critique vis à vis de mon exposé ; faites-vous votre propre opinion ; distinguez les affirmations hasardeuses des informations vérifiables, etc. Et faites-moi part de vos réflexions et de vos critiques (voir l'adresse du préambule).

Le texte écrit, rédigé dans le mois suivant l'exposé oral, en est assez différent (et un peu meilleur, j'espère) ; c'est la conséquence de la lecture de textes de mathématiciens qui approfondissent les liens entre mathématiques et finances. Je reviendrai sur ces différences lors du prochain cours, que j'espère le plus proche possible (note du 31-1-09).

Le contexte de ce cours est tout à fait exceptionnel : la lutte des universitaires et des chercheurs, à laquelle le mouvement étudiant semble se joindre,

pour conserver à l'enseignement universitaire et à la recherche française des qualités que le gouvernement cherche à déstructurer, obsédé qu'il est de vouloir nous imposer les méthodes du libéralisme le plus réactionnaire et utilisant ces derniers temps toute une panoplie de mensonges, erreurs, insultes (au plus haut niveau de l'État) et atermoiements manœuvriers ; c'est pitoyable, cela les disqualifient (à mes yeux), mais je ne sais quand j'écris quelle sera l'issue de ce mouvement. Je noterai juste que le mouvement utilise Internet de façon intense et que les discussions importantes ont lieu des sites du réseau (les réunions à Paris paraissent presque formelles à côté, avec leur défilé de prises de parole comprimées dans un temps trop court). Pour faire fonctionner tout cela, pas mal de mathématiques récentes sont nécessaires.

1.2 La crise de la fin 2008

Attention au sens des mots !

Les sommes concernées sont énormes. Il faut cependant prendre garde au vocabulaire : les mots français billion ($(10^6)^2 = 10^{12}$), trillion ($(10^6)^3 = 10^{18}$) n'ont pas le même sens qu'aux États-Unis où un billion=10^9 est notre milliard, un trillion est notre billion : il y a de quoi s'y perdre ! Quand les deux candidats à l'élection présidentielle américaine débattent, le Monde fait dire à Barack Obama de la dette américaine (Le Monde du 9-10-2008, page 18) qu'elle était : *de 5 trillions de dollars quand George Bush est arrivé et qu'elle dépasse maintenant les 10 trillions* ; il donne une rectification le 18-10-2008, en bas de la page 19. Le système d'appellation des grands nombres 10^{6k} : billions, trillions... octyllions est défini par Nicolas Chuquet (1445/55 à 1488) dans son *Triparty en la science des nombres* resté à l'état de manuscrit. Le système de Chuquet est connu par le plagiat qu'Estienne de la Roche en publie en 1520 : *Larismétique*, sans mentionner Chuquet. Ce n'est qu'en 1870 que le manuscrit de Chuquet fut retrouvé ; il portait des annotations de la main de son plagiaire ! Le mot milliard est dû à Peletier du Mans (1517-1582), poète, humaniste et mathématicien. Le système américain s'est formé autour de 1800.

Des annonces de la catastrophe

La catastrophe fut annoncée, par exemple, par les économistes Nouriel Roubini (université de New York) et Robert Schiller (université de Yale). Une

conférence de Nouriel Roubini en 2006 déchaîna l'hilarité des participants d'une conférence du FMI et ce commentaire narquois du modérateur : *Après cela, il nous faudra un petit remontant* (Le Monde 2, 17-1-2009, page 5). Robert Schiller dit que les grands financiers de la planète sont des personnes aux comportements déterminés par leur milieu social ; ils reprenaient tous l'analyse dominante, ne pouvaient rien critiquer, rien en changer, même si, en leur fors intérieur, certains doutaient de la solidité du système (cette analyse est-elle simpliste ?). Nouriel Roubini et Robert Schiller sont aujourd'hui loués pour leur clairvoyance par la presse américaine, mais aucun grand responsable de la finance ne les avait écoutés.

Le Monde des 25/26 janvier 2009 montre que l'économiste français Maurice Allais a lui aussi averti très clairement des risques que prenaient l'économie mondiale en 1999 dans son livre *La crise mondiale d'aujourd'hui*, aux éditions Clément. Il y parlait des similitudes avec la crise de 1929-1934 ; il était sorti major de Polytechnique en 1929, avait fait un voyage aux États-Unis en 1933. Confronté à la misère, à tous ces Américains qui mendiaient, il avait cherché à comprendre, mais personne ne lui avait paru donner d'explication satisfaisante. Cela l'avait décidé à changer son orientation de recherche, passant de la physique à l'économie pour *promouvoir une efficacité économique aussi grande que possible tout en assurant une répartition des revenus qui soit communément acceptable*. Son livre de 1943 *À la recherche d'une discipline économique* (un millier de pages), lui vaut le prix Nobel en 1988. Dans son livre de 1998, il écrit que, comme en 1929, on constate *la création et la destruction des moyens de paiement par le système du crédit, le financement d'investissements à long terme avec des fonds empruntés à court terme, le développement d'un endettement gigantesque, une spéculation massive sur les actions et les monnaies, un système financier et monétaire fondamentalement instable... Cette instabilité a été considérablement aggravée par la totale libération des mouvements de capitaux dans la plus grande partie du monde... Depuis 1974, une spéculation massive s'est développée à l'échelle mondiale... de gigantesques marchés sur les stock-index-futures*[1], *les hedge*

1. Contrat à terme en français : on vend ou on achète un produit en fixant un prix longtemps à l'avance, pour se protéger des fluctuations des cours (penser à un industriel qui ne souhaite pas que le prix de la matière première qu'il utilise grimpe en flèche subitement) ; cette méthode était déjà appliquée il y a 400 ans ; aujourd'hui, elle s'applique aux produits financiers.

funds[2] *et tous les produits dérivés*[3] *le monde est devenu un vaste casino... L'économie mondiale tout entière repose aujourd'hui sur de gigantesques pyramides de dettes, prenant appui les unes sur les autres dans un équilibre fragile... Jamais sans doute une telle instabilité potentielle n'était apparue avec une telle menace d'un effondrement général.* C'était vraiment bien senti, mais quels financiers pouvaient prêter attention à ces menaces ? Maurice Allais a maintenant 98 ans ; il suit toujours attentivement l'évolution de la crise actuelle et craint que nos hommes politiques ne soient pas à la hauteur.

Je me souviens pour ma part d'articles de journaux se posant sans cesse, ces dernières années, la même question : où va nous mener la dette abyssale des États-Unis ?

L'effondrement

À l'automne 2008, après la crise des subprimes est arrivée une nouvelle crise. Tout le monde prêtant de l'argent à tout le monde dans l'espoir de bénéfices, le système s'est aperçu que certains n'avaient pas l'argent qu'ils étaient supposés avoir et tout s'est écroulé en quelques jours. Les victimes prestigieuses ne manquent pas : une partie des fleurons des bourses de Wall Street et de la City, des noms qui ne disaient quasiment rien pour moi, mais qui jouaient avec des milliards de dollars (à peu près autant en milliards d'euros) : Lehmans brothers, Freddie Mac, etc. L'imbrication des affaires, le fait que chacun doive toujours plein d'argent à plein d'autres, a provoqué par réactions en chaîne des dommages considérables.

L'ancien directeur du SEC (Security and exchange commission), William Donaldson, explique (Le Monde, 13-1-2009), que le SEC, ni aucune autre agence des États-Unis, n'a pu empêcher la création de fonds à haut risque comme les prêts subprimes. Depuis 20 ans, les marchés financiers se sont mondialisés et le marché est devenu de plus en plus complexe, en particulier parce que la distinction entre les banques où on dépose son argent et les banques qui s'occupent des grandes affaires s'est estompée. Il y a vingt ans, aux États-Unis, 4 à 5% seulement des gens avaient des portefeuilles boursiers ; en 2008, une famille sur deux.

Des catastrophes de moindre ampleur sont toujours possibles : par exemple,

2. Fonds d'investissements à haut risque (10 000 environ) avec de l'argent souvent bloqué ; 700% d'augmentation de 1995 à fin 2008, 1500 milliards de dollars y sont placés : le fonctionnement est très opaque, paradis fiscaux hébergeant certains fonds, etc.

3. On peut négocier avec de l'argent qu'on ne possède pas ou pas encore.

les Américains ont souvent 5 ou 6 cartes de crédit, qu'ils utilisent pour différer leurs paiements de plusieurs mois et la crise a augmenté le risque qu'ils ne puissent rembourser un jour le montant total de leurs achats par cartes. Ces derniers jours, on s'aperçoit de l'étendue des dettes des pays d'Europe de l'est ; en Espagne, ne pas payer est un sport national que pratiquent en particulier les communautés urbaines, etc. poussant à la faillite des entreprises.

Le sauvetage miraculeux et nécessaire de certains groupes financiers a eu lieu grâce à de l'argent que les états se sont procurés comme par magie. En fait, ils se sont très lourdement endettés (particulièrement les États-Unis) et on (je) ne peut(x) prévoir où cela va les conduire à moyen terme ; se déclarer eux-mêmes en faillite, faire rembourser par les contribuables modestes les énormes factures de leurs si habiles financiers ? (on s'aperçoit de multiples façons que de l'argent qu'on croyait avoir n'existe plus ou a été récupéré). Nous entrons dans une période particulièrement difficile où tout se rétracte : les entreprises cherchent les économies, les échanges se réduisent. Des conséquences dramatiques vont se multiplier : dans nos pays, la crise va servir de prétexte, les licenciements des plus fragiles, ceux à contrat précaire, comme beaucoup de jeunes, vont se multiplier, le chômage va augmenter ; pour les pays moins armés, il nous est à peu près impossible d'imaginer la détresse (l'aggravation de la détresse plutôt) dans laquelle vont être plongés des milliards d'êtres humains.

1.3 Le scandale Madoff

Le scandale Madoff est une illustration caricaturale de la crise : 50 milliards de dollars (35 milliards d'euros à quelques milliards près, tous ces chiffres sont donnés d'après la presse), le budget de l'éducation nationale en France, se sont volatilisés et personne n'a encore pu déterminer s'il en reste un peu quelque part (un demi-milliard viendrait d'être retrouvé, 7-1-2009) ; à qui le rendre ?).

Bernard Madoff promettait des placements à haut rendement à des investisseurs disposant de gros moyens. Il servait des intérêts substantiels de 8 à 12% avec l'argent apporté par ses clients et le système fonctionnait tant que le nombre de clients augmentait et que peu d'entre eux demandaient le remboursement de leur mise, trop heureux des rendements qui leur étaient offerts. Les clients ne se posaient pas trop de questions sur les méthodes de Madoff, tant qu'ils en bénéficiaient. La chute de Madoff semble être due à

l'arrêt de l'arrivée de nouvel argent due à la crise. Quand suffisamment de clients voulurent retirer leurs fonds, on s'aperçut que les caisses étaient vides.

La chute de Madoff a entraîné des pertes considérables pour de nombreux organismes (dont on ne dit pas le montant des intérêts qu'ils avaient reçus jusque là). On s'aperçoit que l'argent patiemment épargné au cours d'une vie peut d'un seul coup purement et simplement disparaître sans qu'aucun responsable ne puisse être désigné, sinon le système capitaliste actuel lui-même.

Par exemple (Le Monde du 13-1-2009), la banque suisse UBS géraient les fonds LuxAlpha et LuxInvest au Luxembourg et la banque anglaise HSBC le fonds Thema en Irlande. Tout était placé dans les fonds Madoff et il n'en reste rien ; les clients (assez fortunés et demandeurs de ce type de placement) de ces banques cherchent à se retourner contre elles.

La banque Santander est un des fleurons de l'Espagne ; elle était réputé pour le *flair* exceptionnel avec lequel elle plaçait l'argent de ses clients. Elle aurait placé 2,3 milliards d'euros dans les fonds Madoff. Pour garder la confiance de sa clientèle, elle s'apprête à négocier rapidement le remboursement des sommes envolées, entreprenant parallèlement des actions en justice à l'issue plus incertaine.

La banque Medici d'Autriche est touchée dans la même proportion et a perdu tous ses avoirs ; sa directrice, Sonja Kohn, une personnalité flamboyante, se cache par crainte de représailles de ses clients, des oligarques russes. Le record de pertes est détenu par la société de gestion d'actifs Fairfield Greenwich Group : 5,5 milliards d'euros. Plus près de nous, 450 millions de dollars pour Natixis et 350 pour BNP-Paribas, dit-on.

La SEC ne s'était aperçu de rien : ils avaient sans doute eu à consulter des livres de comptes fictifs. Il semble cependant que des avertissements avaient été donnés, par exemple par un certain Harry Markopolos qui avertit la SEC à plusieurs reprises : en 1999, puis dans un rapport très précis du 7-11-2005 (Wall Street journal du 18-12-2008) ; voir Le Monde 2 (17-1-2009, page 5).

Le système semble avoir duré 48 ans. La respectabilité de Bernard Madoff (il a été, en 1990, président du NASDAQ, National Association of Securities Dealers Automated Quotations, le deuxième plus grand marché d'actions du monde après le New York Stock Exchange et le premier pour les entreprises de l'électronique), facilitait la captation des fonds. Mais une fraude de ce type durant autant d'années a sans doute bénéficié de nombreuses complicités ; les enquêteurs ont du travail pour très longtemps, sans qu'on sache si des condamnations seront prononcées un jour (pourquoi pas un non-lieu

quand on aura un peu oublié ?). Bernard Madoff semble avoir demandé à ses fils, membres de sa société, de le dénoncer, afin de les mettre à l'abri des poursuites ; en attendant, il est laissé en liberté !

Ce n'est pas la première escroquerie de ce genre, mais c'est la première à une telle échelle. D'après Wikipedia, Charles Ponzi (1882-1949) devint millionnaire en six mois en 1920 en proposant d'investir dans une spéculation sur les *Coupons réponses internationaux* ; il promettait un rendement de 50% en 45 jours, 100% en 90 jours, et 40 000 personnes investirent 15 millions de dollars de l'époque ; le tiers fut redistribué. On aurait dû se méfier : il avait déjà été en prison pour des faits similaires. Mais il y retourna relativement peu, continuant ses escroqueries ; il est mort pauvre au Brésil, laissant son nom à son système, pauvre gloire posthume.

D'autres schémas de Ponzi sont célèbres : en Albanie, en 1992, le gouvernement autorise la création de banques basées sur cette escroquerie ; leur effondrement, en 1997, cause des milliers de morts. En Colombie, 500 000 personnes ont été victimes de la DRFE : *Dinero rapido, facil y en efectivo*, (en liquide). Enfin, on vient de découvrir début 2009 l'escroquerie du même type de Robert Stanford qui porterait sur 9 milliards de dollars (même si ce n'est pas un record, c'est déjà pas si mal) et touche en particulier les pays d'Amérique latine.

1.4 Le mystère Harpagon

L'argent est absolument nécessaire et plusieurs milliards d'individus aujourd'hui souhaiteraient bien en avoir simplement un minimum pour pouvoir vivre dans des conditions moins difficiles que celles qu'ils connaissent : se procurer un minimum de nourriture pour se nourrir (*manger pour vivre et non pas vivre pour manger* disait Molière), nourrir ses enfants, avoir accès à une habitation minimale avec des conditions d'hygiène correctes, avoir un travail non dégradant, etc.

La gestion de l'argent dans le monde d'aujourd'hui ne s'occupe pas vraiment de ce scandale absolu et qui devrait être insupportable à tous ceux qui s'en aperçoivent (cette idée qui paraît si naturelle est loin d'être universellement partagée). Pourquoi ces grands financiers, ces traders audacieux dont les salaires sont énormes, ne pensent qu'à ces masses d'argent, ne se soucient pas de tous ceux qui n'en ont pas et de leur misère ?

Admirons ces grands classiques pour la création de personnages gardant

leur profondeur et leur mystère des siècles durant. Souvenons-nous de ce que Molière fait dire à Harpagon après le vol de sa cassette par La Flèche : *Mon esprit est troublé, et j'ignore où je suis, qui je suis, et ce que je fais. Hélas, mon pauvre argent, mon pauvre argent, mon cher ami, on m'a privé de toi ; et puisque tu m'es enlevé, j'ai perdu mon support, ma consolation, ma joie, tout est fini pour moi, et je n'ai plus que faire au monde. Sans toi, il m'est impossible de vivre. C'en est fait, je n'en puis plus, je me meurs, je suis mort, je suis enterré. N'y a-t-il personne qui veuille me ressusciter, en me rendant mon cher argent, ou en m'apprenant qui l'a pris ?...Allons vite, des commissaires, des archers, des prévôts, des juges, des gênes*[4]*, des potences, et des bourreaux. Je veux faire pendre tout le monde ; et si je ne retrouve mon argent, je me pendrai moi-même après.*

La convoitise de l'argent se confond avec le goût de la toute puissance et toutes ces manœuvres financières seraient le fait de gens qui ne veulent pas vieillir et cherchent un retour aux jeux de leur enfance en voulant oublier que, pour eux comme chacun d'entre nous, ils disparaîtront un jour, etc.

Tentons encore quelques explications.

La démocratisation des produits financiers a incité beaucoup de gens à chercher un complément à leurs ressources propres. Leurs banquiers se sont bien gardés de leur dire que les produits soi-disant merveilleux qu'ils leur proposaient étaient d'un maniement complexe et que le risque était loin d'être nul. Mais l'espoir de gagner plus en jouant un peu comme dans un jeu d'argent a séduit et toutes les petites sommes drainées ont fait la fortune de quelques uns.

Le goût de l'argent pour l'argent est un comportement social assez général. Dans beaucoup de sociétés, tout ceux qui ont de l'argent trouvent normal d'en parler, de chercher des moyens d'en avoir encore plus. Leurs motivations ne semblent pas avoir leurs racines dans une sorte de syndrome d'Harpagon ; s'ils cherchent à en avoir plus, ce peut être pour se conformer à un modèle social en évolution depuis plusieurs siècles, pour en avoir plus que le voisin, pour mourir avec des possessions, une respectabilité, pour en laisser à leurs enfants, à ceux qui leur sont chers. Ils chercheront une bonne affaire, acheter au bon moment un appartement, des actions ou d'autres produits financiers, un bois, un champ, une maison, jouer avec des déductions astucieuses d'impôt, emprunter plutôt que dépenser l'argent qu'ils ont (ou qu'ils n'ont pas), etc. Ce rapport à l'argent devant toute la misère du monde n'a-t-il pas

4. des tortures.

quelque chose de choquant ? Moi qui écrit ce texte me sens assez mal à l'aise en saisissant ces lignes sur mon Mac, avec mon salaire régulier d'enseignant de l'université. Des milliers de romans sont pleins de ces thèmes.

Enfin, les petites amies de banquiers new-yorkais se trouvent aujourd'hui abandonnées par ceux qui leur offraient quelques moments de luxe et qui sont contraints par la crise à se replier sur leur vie de famille ; elles étaient sûrement séduites par leur argent, mais l'une d'entre elles note sur le blog qu'elles ont créé : *Le banquier est un vrai mâle, agressif, n'acceptant pas qu'on lui refuse quoi que ce soit ; il a confiance en lui, on le respecte et c'est ce qui crée toute la mystique qui l'entoure.* On revient à des comportements d'espèces luttant pour leur survie : les comportements les plus archaïques et les moins civilisés de notre espèce seraient à chercher chez les banquiers et les financiers - :) (je pourrai compléter la liste...).

1.5 L'économie, une science ?

La mondialisation s'est mise en place dans les années Reagan (1980-1988), avec un discours expliquant son inéluctabilité, ses bienfaits économiques. C'était quelques années après la fin des accords de Bretton Woods (voir plus loin). En fait, il s'agissait sans doute surtout, pour ceux qui la promouvaient, les dirigeants des États-Unis et les grands groupes financiers, de faire sauter toutes les entraves à leur liberté à eux, leur laissant la possibilité de se livrer à leurs jeux de concurrence sans entraves et sans frontières où on cherche à bouffer tous ceux qui sont moins forts que vous... tout en se protégeant de possibles prédateurs. Dans ce monde desséché où les batailles financières font rage, les humains du reste de la planète ont tout de même de l'importance : ils doivent produire le maximum de richesses pour permettre ce jeu, travailler au moindre coût, rester sans travail, dans la misère et dans la faim, ou encore consommer en dépensant ce qu'on leur a laissé en achetant des produits dont l'intérêt n'est pas toujours évident. Mais on ne doit pas leur laisser de possibilités de s'organiser et chercher, au contraire, à déstructurer leur tissu social (c'est *mon* interprétation des attaques contre les enseignants et chercheurs en ce moment). Éventuellement, on va même les invité à payer quelque chose pour renflouer ces grands organismes, en présentant cela comme une nécessité pour eux ! Il s'agit d'abord de mondialisation économique, mais on sait bien que les différents aspects de l'activité humaine (culturel, social, sécuritaire, information, recherche...) sont également contrôlés.

Le secrétaire américain au Trésor, Henry Paulson, a été en première ligne ces derniers mois ; son attitude attentiste lui a été reprochée ; il semble être sincère et mis à nu quand il déclare, le 30 décembre 2008 : *Nous n'imaginions pas l'ampleur du mal, nous n'étions pas prêts, nous ne disposions d'aucuns des moyens qui nous auraient été nécessaires.*

Henry Paulson parle bien sûr de moyens d'action qu'on s'était bien gardé de mettre en place au nom du libéralisme, mais il s'agit aussi de bien d'autre chose. On parle volontiers des lois de l'économie, surtout quand c'est pour justifier des refus d'augmentation de salaire. Ces prétendues lois, personne ne les a appliquées, il y a un an, pour prévoir la situation actuelle. Il y a tout lieu de penser qu'elles n'existent pas autrement que dans les incantations pour justifier la mise en place du système ultralibéral qui nous domine.

Nobel n'avait pas prévu de prix en économie, pas plus qu'en mathématiques. Ce prix fut créé en 1970. L'économie se trouvait ainsi reconnue au même titre que la physique ou la chimie. Mais les sujets étudiés par les lauréats ne sont pas de grandes théories économiques, mais le fonctionnement de l'économie dans des domaines particuliers.

Je n'ai pas, pour ma part, l'impression que la science puisse aborder l'étude de l'économie mondiale au niveau global. Une théorie scientifique de l'économie devrait avoir les différentes caractéristiques d'une théorie scientifique, expliquer, prédire, entraîner un consensus. Pour la dernière crise, peu de gens l'ont prédite en donnant des raisons, comme on l'a vu. Leurs analyse ne s'appuyait pas sur des raisonnements pouvant être qualifiés de scientifiques, plutôt leur expérience, les conduisant à penser que la situation économique allait entraîner des conséquences dangereuses, une sorte de raisonnement par analogie. Ils étaient convaincus de ne pas se tromper, mais ils n'ont pas réussi à convaincre d'autres personnes. Nous avons vu que Schiller a une explication : les financiers se seraient refusés, par un comportement panurgique, à admettre des vérités qu'il établissait, lui, rigoureusement.

Mais je vois plusieurs raisons s'opposant à la possibilité d'une théorie scientifique de l'économie, que je conçois comme un modèle mathématique dans lequel on entre des données, des lois, des paramètres de ces lois pour décrire l'évolution du système sur une durée significative. Les sommes en jeu sont gigantesques, bien sûr, mais les acteurs importants ne sont sans doute pas si nombreux que cela. Seulement, les données et les paramètres sont souvent impossibles à connaître : secrets bancaires, mouvements cachés d'énormes capitaux, frauduleux ou non, et surtout : décisions humaines imprévisibles cherchant à faire des coups... (devrait-on parler de meurtres par

métaphore ?)

1.6 Mathématiques et économie

Mouvement brownien

Le Palais de la découverte à Paris, donnait à voir (il y a 50 ans ; le montage existe peut-être encore) le mouvement brownien par un montage très simple : un récipient rempli d'eau dans lequel avait été émulsionné de l'huile en très fines gouttelettes. En regardant la solution au microscope, on voyait les petites gouttes d'huile animées de petits mouvements désordonnés. Ainsi était mise en évidence l'agitation des molécules, un phénomène qui se passait à une échelle beaucoup plus petite, inaccessible à l'observation directe. C'était une évidence visuelle pour quelque chose de difficile à croire possible.

Le mouvement a été observé depuis longtemps ; c'est le biologiste Robert Brown (1773-1858), en étudiant en 1827 des grains de pollen de *Clarkia pulchella* en suspension dans l'eau (ce n'est pas la partie la plus importante de l'œuvre de Brown, mais c'est celle dont on se souvient aujourd'hui) qui lui attribue sa véritable origine (on pensait jusque là à des mouvements dus à des êtres vivants (Brown aurait fait une erreur d'interprétation : les grains qu'il observait auraient été des grains plus petits que les grains de pollen, Brian J. Ford, 1992).

Aujourd'hui, c'est dans les salles de marché qu'on parle du mouvement brownien !

Louis Bachelier (1870-1946)

Louis Bachelier est le grand pionnier. Il montre dans sa thèse : *Théorie de la spéculation*, sous la direction de Poincaré, en 1900, l'utilité du mouvement brownien pour comprendre les phénomènes économiques. Il fait ainsi entrer le mouvement brownien dans le domaine des mathématiques, cinq ans avant le célèbre article d'Einstein. Louis Bachelier a ensuite abordé l'étude des équations différentielles stochastiques, dégageant de nombreuses idées dont l'intérêt n'a été compris que bien plus tard ; certains, comme Paul Lévy, ont cru qu'il s'était trompé ; Kolmogorov a reconnu sa valeur dès 1930. Bachelier a été professeur à Rennes (1925-1927) et il est mort à Saint-Servan. La valeur des travaux de Bachelier est proclamée tardivement par Paul Samuelson (né

en 1915) qui en a fait (1965 et 1973), au prix de changements, la base des mathématiques financières (MF) actuelles. Samuelson a reçu le prix Nobel en 1970 ; c'est un des initiateurs des modèles mathématiques en économie.

Kiyoshi Itô (1915-2008)

Le japonais Kiyoshi Itô (1915-2008) vient de mourir. Il a peut-être été le plus grand probabiliste du dernier siècle. Ses contributions à l'étude des processus stochastiques (ou aléatoires) ont profondément transformé ce domaine. Itô a inventé la notion d'intégrale stochastique et établit des résultats qui en rendent l'usage commode comme la célèbre formule d'Itô (une sorte d'intégration par parties). Je recopie un cours récent de Jean-François Le Gall à Orsay :

La formule d'Itô est l'outil de base du calcul stochastique. Elle montre qu'une fonction de classe C^2 de p semimartingales continues est encore une semimartingale continue, et exprime explicitement la décomposition de cette semimartingale.

Les applications des travaux d'Itô sont nombreuses, particulièrement dans le domaine des MF. Mais ils peuvent aussi servir à étudier le mouvement d'une fusée perturbée par les vents, les turbulences de l'écoulement de l'air ou les vibrations de ses moteurs.

On se souviendra de Michel Métivier, professeur à la faculté des sciences pendant les années 1960-70 qui avait orienté une partie des recherches de ses élèves sur le calcul stochastique.

L'économie mondiale après la guerre de 1939-1945

Les deux paragraphes suivants cherchent à suivre (le moins mal possible) un exposé de Nicole El Karoui. Les accords de Bretton Woods, signés aux États-Unis le 22 juillet 1944, organisaient l'économie mondiale de l'après guerre (le britannique John Keynes et l'américain Harry White sont les figures centrales de cet accord) ; c'est alors que sont créés la Banque mondiale et le Fonds monétaire international (FMI). Les accords prévoient que le dollar américain doit jouer un rôle prépondérant, mais il est rattaché à la valeur de l'or.

Au début des années 1960, les dépenses de la guerre du Viet Nam provoquent l'afflux massif de dollars dans des pays (comme l'Allemagne) qui exportent vers les États-Unis. Quand ces pays demandent le remboursement

de leurs dollars en or américain, les Américains suspendent la convertibilité du dollar en or afin de ne pas perdre leurs réserves (le 15 août 1971). Le système des taux de change fixe s'écroule en mars 1973. Les accords de Bretton Woods sont caducs.

Pour l'Europe, c'est le début d'une longue marche vers une monnaie unique pour éviter les effets désastreux de monnaies aux taux fluctuants (en particulier sur les produits agricoles).

La formule de Black-Scholes (1973)

Vers 1973, l'économie devient donc libre : les taux de change, les taux d'intérêt, les cours des actions varient plus rapidement d'un jur à l'autre, d'un mois à l'autre. Les moyens informatiques et techniques permettent une communication de plus en plus rapide des informations et des ordres à travers le monde et les marchés financiers sont ouverts presque 24 heures sur 24.

Les entreprises, en particuliers les grandes, sont confrontées à des problèmes de risques : elles achètent, elles empruntent, elles vendent en dollars ou en une autre devise et les paiements ont lieu quelques mois plus tard. Comment peuvent-elles se protéger contre les risques de pertes qu'elles encourent quand le marché fluctue tous les jours, avec des mouvements d'amplitude plus longue (penser au mouvement brownien) ? Le premier marché des risques financiers ouvre à Chicago vers 1972-73, d'autre se sont ouverts depuis. Les banques propose un nouveau service : garantir une sorte de prix minimum à l'échéance de quelques mois, avec participation aux bénéfices s'il en apparaît (La Poste s'y est essayé en 1999 et la crise de l'époque a provoqué des pertes sensibles de petits épargnants).

La méthode de Black-Scholes introduit une méthodologie révolutionnaire et c'est toujours la référence sur le marché des options. Avec l'argent qui lui est versé initialement, elle propose une stratégie dynamique permettant de réduire le risque final inhérent. Il faut mettre au point un modèle mathématique raisonnable dont le but n'est pas d'estimer les pertes potentielles, mais de les réduire en suivant au jour le jour au plus près les fluctuations du marché. C'est là que le calcul stochastique mis au point par les mathématiciens trouve à s'appliquer.

La formule de Black-Scholes est due à Fischer Black (1938-1995), Myron Scholes (né en 1941) ; elle a aussi été étudiée par Robert Merton (né en 1944). Le prix Nobel a récompensé Merton et Scholes en 1997, rendant hommage à Black, mort peu de temps auparavant. Notons que le *Hedge fund* fondé en

1994 par Merton et Scholes était en faillite quatre ans plus tard ! (à cause d'erreurs qui ne remettraient pas en cause le modèle, dit Nicole el Karoui)

Les modèles mathématiques

Le développement des mathématiques financières de ces vingt dernières années s'appuie sur toutes ces avancées ; sa réussite vient de ce que les recherches sont fortement liées aux techniques bancaires actuelles. mais leur application est très délicate en principe : beaucoup de choses sont inconnues, les paramètres sont difficiles à estimer, etc.

Les années 1970 ont vu l'élaboration de modèles en économie où la théorie des probabilités était essentielle. Après la crise de 1987, les financiers ont été demandeurs de formations mathématiques. La puissance des ordinateurs s'accroissait rapidement et l'apparition de microordinateurs en réseaux a transformé les possibilités de calcul et d'action.

Marc Yor

Marc Yor est né en 1949. Il est professeur à Paris 6 depuis 1981, membre de l'Académie des sciences depuis 2003. Il dirige l'équipe de recherches : *Mouvement brownien et calcul stochastique*. Marc Yor a présenté lui-même ses recherches (voir le site http ://www.academie-sciences.fr/membres/discours_pdf/notice_Yor.pdf) en les classant sous 20 thèmes étroitement imbriqués. Il lui arrive de signaler des applications aux mathématiques financières.

En 2005, Marc Yor a organisé à l'Académie des sciences une journée de conférences sur les mathématiques financières, dont on peut trouver les vidéos sur le site http ://www.academie-sciences.fr/conferences/seances_publiques/html/debat_01_02_
En voici les auteurs et les titres.

1) Marc Yor : Introduction.

2) Hans Föllmer : Incertitude financière, préférences et mesures de risque.

3) Walter Schachermayer : Introduction aux notions d'arbitrage / Qu'est-ce qu'un Free Lunch ?

4) Nicole El Karoui : Un Marché dynamique du risque / Le Monde des produits dérivés.

5) Hélyette Geman : Horloge stochastique et marchés financiers.

6) Damien Lamberton : Options et équations aux dérivées partielles.

7) Emmanuel Gobet et Gilles Pagès : Bilan temporaire et conclusions de la journée.

1.7 Le point de vue de Denis Guedj dans Libération,

L'article date du 10 décembre 2008. Denis Guedj souligne d'abord le statut des mathématiques financières ; elles ne feraient pas partie des grandes branches des mathématiques comme la théorie des nombres, la géométrie algébrique, les probabilités. Ce ne serait qu'une application d'une petite partie des mathématiques, sans grand problème à résoudre.

Jusqu'ici, les applications des mathématiques pouvaient avoir leurs aspects bénéfiques et leurs aspects négatifs pour la société. Les MF sont au service de ceux qui recherchent des gains, les grands organismes financiers internationaux. Elles n'ont jamais été conçues pour apporter du bien-être à ceux qui souffrent.

Les MF sont un instrument de puissance aux mains des jeunes (on parle de *quants*, quantitative people) sortis des formations spécialisées. Denis Guedj souligne que ces quants sont *au mieux dans une inconscience polissonne, au pire dans un cynisme condamnable* ; Michel Rocard pense, lui, que leur action peut être qualifiée de *crime contre l'humanité* (je ne peux m'empêcher de dire tout de suite que je trouve que l'ancien premier ministre tombe un peu trop dans la facilité de formules chocs !). Les jeunes étudiants en mathématiques qui s'engage dans l'étude des MF espèrent de gros salaires ; on peut dire qu'ils sont organisés en bandes et qu'ils travaillent au malheur du plus grand nombre ; ce sont des ennemis objectifs ; ils dépouillent peu à peu les institutions démocratiques de leur pouvoir ; au sens strict du terme, ce sont des terroristes (c'est Denis Guedg qui parle).

Si les quants ont été formés pour la gestion des risques, nous devons les applaudir très fort : avec tout leur bagage théorique, ils n'ont pas du tout vu venir la crise et ont continué jusqu'au dernier moment leurs activités.

La fin de l'article de Denis Guedj est consacrée à Madame Karoui, *Laure Manaudou de la finance* : elle a osé affirmer que *les MF n'ont rien à voir avec la crise*. Denis Guedj en attend une démonstration mathématique rigoureuse.

Les salaires des doctorants en mathématiques sont dérisoires par rapport à ceux des quants : au moins dix fois plus pour les quants, 100 à 150 mille euros par an (sans compter d'éventuelles primes).

Denis Guedj rappelle la phrase de Georg Cantor : *L'essence des mathématiques est la liberté* et conclut : *Une fête des mathématiques d'un côté, des mathématiques mercenaires de l'autre.*

1.8 Le point de vue de mathématiciens

Jean-Pierre Bourguignon

Jean-Pierre Bourguignon est l'actuel directeur de l'IHES.

Il souligne que le rôle des mathématiciens dans le domaine de la finance date d'une vingtaine d'années et est devenu très important. Les élèves de Nicole El Karoui (qui dirige, avec Gilles Pagès et Marc Yor, le DESS commun à Paris VI et à l'X) ont un grand succès et le Wall Street Journal l'a mise en première page.

Le développement des MF répond à un besoin d'avoir des outils d'estimation et de décision ; les possibilités de calcul des ordinateurs permettent de tester des modèles de plus en plus complexes. Les objectifs, comme la rentabilité, sont ceux des banquiers, les méthodes, comme le recours à l'emprunt, sont les leurs. Les quants sont parmi les plus doués des mathématiciens actuels ; ils choisissent ces carrières, au détriment d'autres, pour les salaires élevés qui leur sont proposés.

Ceux qui sont responsables de la crise sont ceux qui ont fait le choix du surendettement, du refus de savoir ; il a pu y avoir des mathématiciens parmi eux, mais ce n'est pas en tant que mathématiciens qu'ils sont responsables.

Jean-Pierre Bourguignon cite le cas de mathématiciens ayant attirer l'attention des dirigeants sur les risques globaux de ces dernières années et dit que l'un d'eux a été prié de quitter son établissement.

Les banques veulent conserver le secret sur leurs données et le travail mathématique est très souvent parcellisée et ne donne pas la possibilité de recherches sérieuses.

Stéphane Jaffard

Stéphane Jaffard est professeur à Paris 12 et président de la SMF (Société mathématique de France). Il y a 20 ans, les mathématiciens travaillaient sur des modèles bien limités. Leur travail a changé de nature depuis. Les mathématiciens ne peuvent pas aboutir à des résultats solides car leurs travaux sont basés sur des hypothèses difficiles à évaluer :

- des hypothèses qualitatives sur le marché, comme on ne peut gagner sans prendre de risques, d'où l'importance du calcul stochastique, mais ce calcul est difficile à appliquer dans ce contexte, comme la mécanique des fluides est difficile à appliquer au trafic routier ;

- des hypothèses quantitatives pour fixer la valeur des paramètres du modèle, sur leurs lois d'évolution ; un analyste financier aura tendance à utiliser le modèle dans des conditions limites, voire pire, suivant son intuition qui peut être défaillante ;

- des hypothèses de phase régulière dans les activités économiques ; les modèles ne sont pas faits pour les situations de crise. Ce qui me rappelle deux choses. Quand j'étais, avec mon épouse, en 1970, à l'Université centrale de Caracas, elle avait eu l'occasion de se faire expliquer un modèle de la vie politique au Vénzuéla ; une sortie *coup d'état* était prévue ! Autre chose : la tempête d'octobre 1987 en Bretagne est restée dans toutes les mémoires ; certaines villes paraissaient totalement sinistrées, etc. : les modèles de l'époque n'avaient pas prévus la tempête parce que leur conception ne le permettait pas ; ce sont les météorologues humains qui, au vu des données, comprirent qu'un événement exceptionnel se préparait et donnèrent l'alerte, permettant de s'organiser quelques heures avant les grandes rafales de vent ; la confiance dans la modèle était plus forte en Angleterre et la tempête surprit terriblement les Anglais.

Certains mathématiciens sont horrifiés de l'utilisation qui est faite de leurs modèles, dit Stéphane Jaffard. Les banquiers utilisent les modèles en boîte noire, sans recul critique, dans des conditions hors de leurs limites. Dans beaucoup de problèmes financiers, les modèles ne sont pas encore construits.

Marc Yor

Nous avons déjà dit que Marc Yor enseignait dans le master de probabilités et finances de Paris 6, avec Nicole El Karoui et Gilles Pagés. Il esquisse, dans le bulletin de la SMF, une réponse aux propos de Michel Rocard. Les mathématiciens ont été impliqués dans la création de nouveaux produits financiers sophistiqués. Mais la dérive des quinze dernières années : fonds incontrôlés, marché de l'immobilier contrôlé par les banques, subprimes, résulte de décision de banquiers et non de mathématiciens. Le rôle des mathématiciens serait de comprendre les phénomènes financiers et éventuellement, de dénoncer des produits dangereux. Marc Yor demande aussi un numerus clausus pour les quants, afin d'orienter de très bons étudiants vers d'autres domaines.

Antoine Paille

Antoine Paille qui, parmi d'autres activités, travaille à la Société générale, a été questionné par le Figaro du 31 octobre 2008. Il explique que les mathématiciens ont permis la gestion du risque et le calcul des rendements possibles. On demande aux mathématiciens de fabriquer des modèles pour des salles de marché ; on ne leur demande pas d'étudier les hypothèses sous lesquels est conçu ce modèle.

La France a imposé sont point de vue dans certains domaines qui ne se sont pas effondrés à l'automne. Le domaine qui s'est effondré est le domaine du crédit, un domaine construit par les Américains, de plus en plus opaque, très concentré dans les mains d'opérateurs américains. Le marché mondial du crédit a été absorbé par le financement de l'accès au logement des ménages américains. Antoine Paille insiste sur cette concentration qui interdit toute solution de secours en cas de difficulté majeure. Il insiste aussi sur l'opacité, qui permet toutes les manipulations, sur l'évaluation des risques, basée sur des critères des années 1990, alors que des initiatives imprudentes se multipliaient. Les conditions des marchés ont finis par s'écarter complètement des modèles mathématiques (j'ajoute : ce dont les financiers se moquaient probablement) jusqu'à ce que le marché américain du crédit s'écroule.

Embauches

Les sociétés spécialisées recrutent toujours des jeunes thésards. Le Monde cite le cas d'une jeune femme, expliquant que les banques lui confie des missions de création de modèles mathématiques pour définir les prix des produits dérivés, en évaluer le coût, etc. Elle emploie une cinquantaine de consultants aussi bons mathématiciens que connaisseurs des produits financiers complexes et de l'informatique ; elle en recrute deux ou trois par mois. Le salaire de départ est de 50000 euros annuels, bruts très probablement.

Le directeur du programme doctoral de l'université Columbia de Chicago reconnaît que les Français sont très réputés et que la compétence est indispensable.

Ivar Ekeland indique que la finance de marché n'offre qu'une partie des emplois possibles et qu'il faut gérer bien d'autres choses, le pétrole et les autres ressources non renouvelables.

Le vice-président de l'université Dauphine souligne que *les docteurs en finance n'ont pas d'inquiétude à avoir*, car si certains mettent en cause les

modèles, on a en réalité *besoin de mieux comprendre*. Les excès ont été commis par ceux qui ont manqué de distance vis à vis des modèles. La célèbre Nicole El-Karoui va dans le même sens : *il faut éduquer l'ensemble du management aux limites des modèles, à l'analyse des risques, car quand un secteur affiche une rentabilité nettement supérieure au reste, les effets sont toujours les mêmes : on investit de plus en plus et on ne maintient pas de regard critique.*

Remarques finales

Pour compléter ces notes de lecture, j'ajouterai deux ou trois remarques.

Les financiers demandent aux mathématiciens de travailler sur des modèles correspondant à leur idéologie libérale. N'y aurait-il pas d'autres perspectives de travail pour les mathématiques financières ?

Il me semble clair aussi que les mathématiciens en général n'ont probablement pas grand chose à voir avec la crise : ils travaillent pour comprendre à un certain niveau, pour modéliser des activités financières à un niveau plus technique. Constamment, ils sont face à des décisions qui ne tiennent aucun compte de leurs modèles, à une opacité du système qui les empêche de créer des modèles ou de déterminer correctement les paramètres des lois qu'ils mettent en œuvre.

Si certains mathématiciens ont joué de leur virtuosité technique pour réaliser des *coups* (pas toujours réussis d'ailleurs), penser à s'enrichir sans voir les conséquences de leurs actes, on peut reprendre les phrases de Denis Guedj pour les condamner.

Il semble enfin que les mathématiciens de la finance soient tous formés sur le même moule. Même très brillants, leurs idées doivent être assez proches. Ne peut-on imaginer qu'ils obtiennent à peu près tous les mêmes résultats et que, dans un environnement économique stable, leur rôle serait plutôt d'être là pour signaler les initiatives dangereuses d'un financier ?

Chapitre 2

Préhistoire

Ce chapitre doit beaucoup aux travaux d'Olivier Keller, en particulier au texte d'une intervention au colloque IREM du 20 juin 2002 à l'ENS de Lyon.

2.1 Du côté de l'archéologie

Que connait-on de la préhistoire ? Beaucoup d'ossements, de restes de camps, de cailloux plus ou moins finement éclatés et taillés, quelques grottes célèbres avec des peintures, Altamira près de Santander en Espagne, Lascaux dans le Périgord, etc. Mais dans tout cela, quoi de mathématique ? Rien, ou plutôt, de très rares objets dont le caractère mathématique n'est pas évident du tout.

Le plus ancien peut-être, daté de -35 000 ans, est un péroné de babouin découvert dans une grotte des montagnes Lebombo du Swaziland, sur lequel ont été incisées 29 traits ; on est tout de suite alerté : s'il s'agissait de 29 jours, on pourrait penser à un calendrier lunaire ?

L'os d'Ishango, encore un péroné, trouvé sur le bord nord du lac Édouard, au Zaïre près de la frontière avec l'Ouganda, est daté de -22 000 ans. Il est beaucoup plus intrigant. Il comporte trois séries de traits marquées sur trois faces de l'os (la figure est de D. Huylebrouck). Je suppose que les premiers découvreurs n'étaient pas des mathématiciens, ce qui expliquerait leurs délires. Par exemple, une face donne les quatre nombres premiers entre 10 et 20, ou encore elle porte la trace d'une numération de base $a = 12$ en donnant $a-1, a+1$ et $3a/2-1, 3a/2+1$, etc. et les sommes des deux autres colonnes sont 48 et 60. Olivier Keller, après avoir démoli la pertinence de ces rappro-

chements donne un exemple amusant : certaines femmes africaines font de temps à autre une encoche sur leur cuiller en bois. S'agit-il d'observations sur les nombres premiers, sur des cycles lunaires... ? Pas du tout : elles notent simplement le nombre de fois que leur mari leur a tapé dessus ; quand il n'est plus possible de tracer une nouvelle encoche, elles lui demandent de s'en aller. Pourquoi l'os d'Ishango ne serait-il pas un témoignage des brutalités des maris il y a 22 000 ans ?

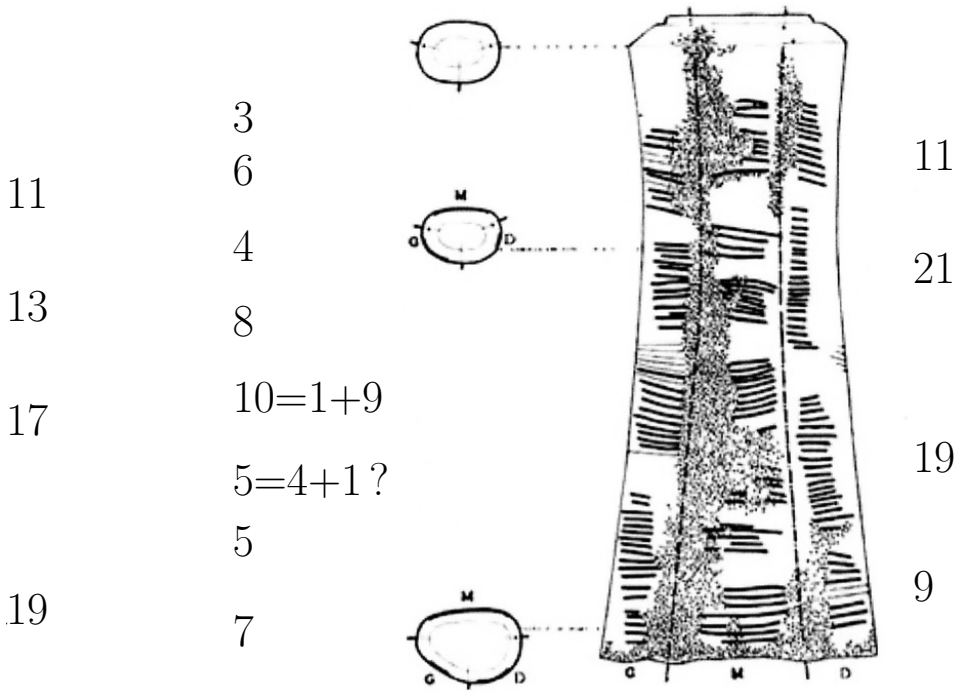


FIGURE 2.1 – L'os d'Ishango.

2.2 Du côté de l'ethnologie

Faute de pouvoir reconstituer les notions relevant des mathématiques de la préhistoire, on peut envisager de s'en faire une idée en étudiant les peuples dits primitifs qui vivent encore actuellement dans différentes régions

du monde. On aura une vision, déformée sans doute, mais quoi faire d'autre de ce qui a pu être pensé pendant la préhistoire.

Nous allons juste parler des systèmes de numération.

Des systèmes de numération de tribus amazoniennes indiquent des stades différents de maîtrise des nombres.

Les Mundurukus, membres d'une tribu amazonienne du Brésil étudiée récemment par Pierre Pica et d'autres, comptent jusqu'à 4 ou 5 et sont incapables de soustraire 4 de 6. Cependant, les enfants mundurukus et américains ont les mêmes résultats dans des tests de comparaison de nombres de points (plusieurs dizaines) dans des images ou dans des tests de géométrie. À partir de ces compétences qui seraient en chacun de nous, les mundurukus n'auraient pas encore inventé le minimum d'outils de langage pour calculer exactement : ils n'auraient pas de mot pour des nombres exacts comme 10, 11, 12... mais plutôt des mots pour dizaine, vingtaine, trentaine.

Des comparaisons d'Olivier Keller entre des systèmes de dénomination des nombres entiers petits sont évocatrices de ce qu'a pu être une évolution de systèmes primitifs de base 5 (doigts-main) vers un système à base 10 (mains-pieds) ou à base 20 (mains-pieds-indiens).

Par exemple, les Zunis, qui vivent au nord du Nouveau Mexique, n'ont pas de nom spécial pour les petits nombres et ne peuvent pas aller facilement au-delà de 10.

Zunis	
1	pris pour commencer
2	levé avec le précédent
3	le doigt qui divise également
4	tous les doigts levés sauf un
5	l'entaillé
6	un autre ajouté à ce qui est déjà compté
7	deux amenés et levés avec le reste
10	tous les doigts
11	tous les doigts et un en plus levés

On voit que 10 ne joue pas pour les Zunis un rôle d'unité pour compter de plus grands nombres

Des indiens du Paraguay n'ont pas cette difficulté et peuvent aller jusqu'à 20 sans difficulté.

Paraguay	
1	mot spécial
2	mot spécial
3	composé de un et deux
4	les deux côtés pareils
5	une main
6	un autre ajouté
10	tous les doigts
11	arrivé au pied, un
16	arrivé à l'autre pied, un
20	fini les pieds

Arrivés à 20, ces Indiens sont un peu devant le même problème que les Zunis quand ils arrivent à 10.

Un système plus évolué se rencontre chez les Tamanac du Vénézuéla.

Tamanac	
1	mot spécial
2	mot spécial
3	mot spécial
4	mot spécial
5	une main entière
6	un de l'autre main
9	quatre de l'autre main
10	les deux mains
11	un du pied
15	tout un pied
16	un de l'autre pied
20	un indien

Faire correspondre un indien au nombre 20 permet de compter facilement beaucoup plus loin : on va chercher un copain : 21 = un des mains d'un autre indien, 40=deux indiens, etc. Ce système semble expliquer la fortune de la base 20. D'ailleurs, il en reste quelques traces dans notre langue : quatre-vingts dans nos noms de nombres, six-vingts dans Molière, l'hôpital des Quinze-Vingts à Paris.

Certains ne vont pas beaucoup plus loin : il n'y aurait rien à compter avec, alors, à quoi ça servirait ? Des Papous (les Iqwaye) vont jusqu'à 500 en

base 20, avec des noms de plus en plus longs, ce qui rend les calculs difficiles : 500=autant de personnes que moi et la main d'une autre personne (20+5) avec leurs mains et leurs jambes, soit $25 \times 20 = 500$; des nombres de la forme $k \times 20 + 10 + l$ avec $1 \leqslant k < 19$, $l = 6, 7, 8, 9$ sont encore plus sportifs.

Notons des curiosités : les Yukis, un peuple indien de Californie dont il ne reste que peu de représentants, comptaient avec les espaces entre les doigts, dans un système de base 8 ; des Népalais, des Africains comptent en base 12. Les Yorubas utilisent la soustraction de 15 à 19 : $15 = 20 - 5$, $16 = 20 - 4$ et pour 50= trois vingtaines moins dix...

Les chasseurs-cueilleurs n'auraient pas eu besoin de développer leur usage des nombres ; c'est le cas par exemple des aborigènes australiens. Plus un peuple commence à pratiquer un peu d'agriculture ou d'élevage, plus le besoin des dénombrements précis le conduisent à développer une numération efficace. Olivier Keller donne de nombreux exemples. Il a aussi écrit sur la géométrie avec la même démarche. Il est cependant temps de clore ce petit chapitre.

Chapitre 3

Mathématiques babyloniennes

3.1 Le système sumérien de numération

La civilisation sumérienne qui se développe au troisième millénaire avant J.C., en Mésopotamie (entre les deux fleuves, fleuve=*potamos* en grec), a produit des œuvres merveilleuses, aussi bien littéraires qu'artistiques ; voir, par exemple, les livres de Samuel Noah Kramer, Jean Bottéro, André Parrot. Les sumériens écrivaient avec un *calame* (tige de roseau) sur des tablettes d'argile fraîche qu'ils faisaient ensuite sécher au soleil et qui nous sont parvenues telles qu'elles avaient été écrites ou recopiées ; il y a très peu de pierres en Mésopotamie. Malheureusement, le travail des archéologues est terriblement menacé depuis le printemps 2003, quand, sous les yeux de l'armée américaine passive, le musée de Bagdad et les sites de fouille de l'Irak ont été pillés pour alimenter le commerce clandestin des antiquités (les photos de sites pillés sont impressionnantes).

Les toutes premières tablettes, datées de -3300 (les débuts de l'agriculture au Moyen-Orient datent des années -11 000), marquent une étape cruciale de la naissance de l'écriture. L'étape précédente est celle des bulles-enveloppes, petites sphères d'argile de 3 centimètres dans lesquelles on plaçait des jetons (on retrouve pendant plusieurs millénaires un nombre considérable de jetons dans les fouilles de niveaux anciens), puis sur laquelle on inscrivait quelques signes pour garder la mémoire d'un accord.

Les premiers coups de génie ont été de supprimer les jetons, d'aplatir les bulles et de développer l'écriture. Les premières tablettes sont par exemple, des décomptes de béliers, brebis, agneaux et agnelles. La naissance de l'écriture

FIGURE 3.1 – Bulle-enveloppe et jetons.

est liée à l'écriture de nombres ; elle n'est pas encore linéaire.

Les différents systèmes de mesure propres à chaque ville et à chaque domaine de mesure s'unifient vers -2100, sans doute sous le règne de Naram Sin ; un système de numération en base 60 s'impose, réduit à deux signes qui suffisaient pour tout écrire, un clou et un chevron, obtenus en appuyant différemment le calame sur la tablette.

FIGURE 3.2 – Le clou et le chevron.

Pour écrire 56, on écrira 5 chevrons suivis de 6 clous (les chevrons sont emboîtés, les clous regroupés par 3 si besoin). Pour écrire $6975 = 3600 + 56 \times 60 + 15$, on écrit un clou, puis 56, puis 15 (un chevron et 5 clous). Le clou vaut donc 1 ou, plus généralement, 60^k, le chevron vaut 10 ou, plus généralement, 10×60^k avec $k \in \mathbb{Z}$, sans que rien ne permette souvent de connaître l'ordre de grandeur. Pour écrire 3 615, on écrit un clou, puis 15 ; le scribe laisse

parfois un espace, parfois non ; il faut deviner. Ce n'est que bien plus tard, vers -300, qu'on trouve dans des tablettes une notation de séparation jouant le rôle de notre zéro comme dans l'écriture de l'année de publication de ce livre : 2008.

Le système en base 60 se diffuse chez les mathématiciens grecs dans les années -300 ; il sera transmis par les Arabes aux Européens et, si vous regardez votre montre en me lisant, vous devriez avoir une pensée pour le, ou les, mathématicien(ne)s qui ont inventé ce système il y a plus de 4000 ans.

3.2 Un calcul dans le système d'unités babyloniens

2 ŠE 1/12 le volume
2/3 de la longueur : la largeur
1/2 de la largeur : la hauteur
la longueur, la largeur, la hauteur, tu croises
puis tu dénoues son inverse
puis à son volume tu élèves
le côté de 15 37 30 est à extraire
le côté est 2 30
la longueur : 15 šu-si
la largeur : 10 šu-si
la hauteur : 5 šu-si

Il faut bien sûr interprèter le texte : il s'agit d'un parallélépipède dont on donne le volume V et des relations entre sa longueur L, sa largeur l, sa hauteur h qui permettent de les déterminer.

Nous pouvons faire un calcul algébrique :
$l = 2L/3$, $h = l/2 = L/3$, $V = Llh = 2L^3/9$, d'où $L = \sqrt[3]{9V/2}$.

La simplicité algébrique du problème est compliquée par le système d'unités, même s'il a été unifié.

Unités de longueur

1. 1 šu-si = 6 še, environ 1,65 centimètres, un doigt ;
2. 1 kùš = 30 šu-si environ 50 centimètres, une coudée ;
3. 1 gar = 12 kùš=6 00 su-si ; on dit aussi ninda ;

4. 1 eše = 10 gar ;
5. 1 uš = 6 eše ;
6. 1 danna = 30 uš, près de 11 kilomètres.

Unités d'aire

1. 1 gin = 180 še ;
2. 1 sar = 1 gar^2 = 60 gin, environ 36 mètres carrés ;
3. 1 iku = 100 sar ;
4. 1 eše = 6 iku ;
5. 1 bur = 3 eše.

Unités de volume

Les unités de volume correspondent aux unités d'aire : on prend un parallélépipède de base une des unités d'aire et de hauteur 1 kùš, quelle que soit l'unité d'aire. Nous les noterons avec les noms des unités d'aire écrits en majuscules.

Revenons au problème.

On connaît le volume V en ŠE.

Comme 1ŠE=$\frac{1}{180}$GIN, que 1 GIN=$\frac{1}{60}$ GAR et que
1 GAR=1 ninda^2×1 kùš,

on a V =2 ŠE 1/12=$\frac{25}{60 \times 180 \times 12}$ GAR.

Comme le volume de 1 GAR est un volume de 1 ninda^2×1 kùš=$\frac{1}{12}$ninda^3, on voit que, si on exprime L, l, h en ninda, on a

$2L^3/9 = \frac{25}{60 \times 180 \times 12^2}$, soit $L^3 = \frac{125}{60^3 \times 8}$.

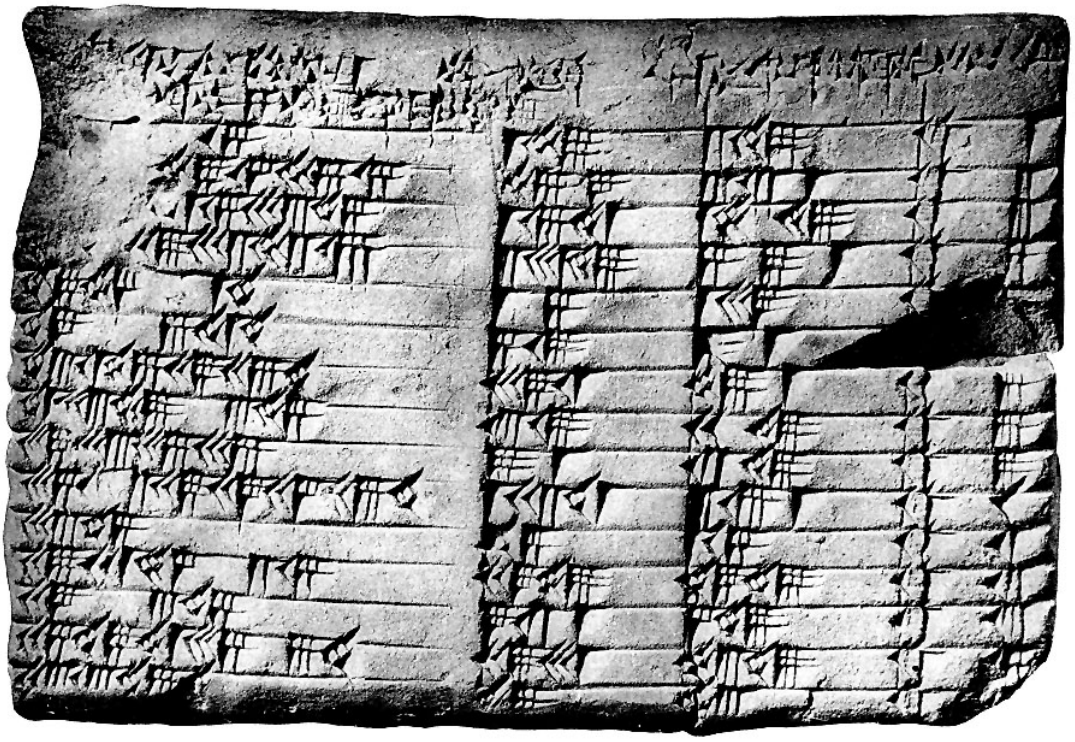
Pour nous, il est facile d'en déduire $L = \frac{5}{60 \times 2} = \frac{1}{60}(2\ 30)$, puisque 125 et 8 sont des cubes.

Mais le scribe babyloniens calcule d'abord 125/8=15 37 30 (le seul nombre donné dans la solution de la tablette), puis la racine cubique de ce dernier nombre.

Il reste à convertir les 2 30 soixantièmes de ninda en šu-si (multiplier par 12×30) pour obtenir $L = 15$ šu-si et conclure.

On a remarqué que ces valeurs étaient les dimensions de la brique de l'époque.

3.3 Plimpton 322



Présentation de la tablette

La tablette Plimpton 322 est une tablette babylonienne de 12,7 sur 8,8 centimètres, provenant d'une fouille clandestine, probablement à Larsa, au sud de l'Irak actuel, et portant le numéro 322 dans la collection laissée à l'université Columbia de New York par George Plimpton. Elle daterait des années -1800 et a été victime d'une cassure à gauche. Elle a été déchiffrée et analysée pour la première fois par Otto Neugebauer (1899-1990) et Abraham Sachs (1914-1983) en 1945 [1] ; Plimpton pensait qu'il s'agissait d'une tablette

1. Voir Neugebauer et Sachs, *Mathematical cuneiform texts*, American oriental series 29, 1945 (et non Neugebauer seul en 1951, comme le dit Wikipedia.

commerciale. L'analyse de Sachs et Neugebauer donne à la tablette un caractère exceptionnel. Eleanor Robson a proposé en 2001 une interprétation qui rend, selon elle, la tablette plus banale ; elle ne m'a pas convaincu : elle suppose que l'auteur sumérien aurait suivit une autre démarche, mais le choix final des nombres aurait été fait avec des critères très artificiels.

c^2/b^2	a	c	n° de ligne
[1 59 00] 15	1 59	2 49	1
[1 56 56] 58 14 50 06 15	56 07	3 12 1*	2
[1 55 07] 41 15 33 45	1 16 41	1 50 49	3
[1] 5[3] [1]0 29 32 52 16	3 31 49	5 9 1	4
[1] 48 54 01 40	1 05	1 37	5
[1] 47 06 41 40	5 19	8 01	6
[1] 43 11 56 28 26 40	38 11	59 01	7
[1] 41 33 59 03 45*	13 19	20 49	8
[1] 38 33 36 36	9 01*	12 49	9
[1] 35 10 02 28 27 24 26 40	1 22 41	2 16 1	10
[1] 33 45	45	1 15	11
[1] 29 21 54 02 15	27 59	48 49	12
[1] 27 00 03 45	7 12 01*	4 49	13
[1] 25 48 51 35 06 40	29 31	53 49	14
[1] 23 13 46 40	56	53*	15

FIGURE 3.3 – Les chiffres lisibles sur la tablette de la tablette Plimpton 322.

Les titres des colonnes conduisent à considérer a et c comme un côté de l'angle droit et l'hypoténuse d'un triangle rectangle à côtés entiers : on peut vérifier pour 11 des 15 lignes (celles sans *) que le troisième côté de l'angle droit, $b = \sqrt{c^2 - a^2}$ est aussi entier. Par exemple, ligne 7, on a $a = 38 \times 60 + 11 = 2291$, $c = 59 \times 60 + 1 = 3541$ et $b = \sqrt{3541^2 - 2291^2} = 2700$.

Les triplets (a, b, c) définissant un triangle rectangle à côté entiers a, b, c, avec c pour l'hypoténuse, sont appelés *triplets pythagoriciens*.

On peut corriger les nombres marqués d'une * dans les 4 lignes erronées, par exemple, le 9 01 de la ligne 9 doit être corrigé en 8 01=481. Les chiffres entre crochets ne sont plus visibles sur la tablette ; les 1 de la première lignes ne sont pas sûrs ; leur présence pourrait expliquer la cassure de la tablette à cet endroit. La ligne 11 correspond au triangle $(3, 4, 5)$.

Comment les Babyloniens en étaient-ils arrivés là ? Neugebauer et Sachs pensaient qu'ils avaient trouvé d'une manière ou d'une autre que les triplets $a = k(m^2 - n^2), b = 2kmn, c = k(m^2 + n^2)$ sont pythagoriciens pour k, m et n entiers ; on peut imaginer, mais cela ne prouve rien, que la formule $(a + b)^2 = (a - b)^2 + 4ab$ peut le suggérer. Un argument renforcerait la thèse de Neugebauer et Sachs : la liste des triplets donnés par ces formules, avec m et n réguliers (c'est-à-dire n'ayant que 2, 3, 5 comme diviseurs premiers, afin que leur inverse en base 60 ait un développement fini), premiers entre eux et inférieurs à 125 et le plus petit angle du triangle entre 32 et 45 degrés est exactement celle de la tablette.

Nous allons détailler ces affirmations. D'abord la démonstration du théorème donnant tous les triplets pythagoriciens.

Théorème

Les triplets d'entiers a, b, c vérifiant $a^2 + b^2 = c^2$ sont tous, à l'ordre près, de cette forme.

Démonstration

1) On peut tout d'abord se ramener au cas où le pgcd de a, b, c est égal à 1, car, en notant k ce pgcd, le triplet $(a/k, b/k, c/k)$ est lui aussi un triplet pythagoricien.

2) On remarque alors que a et b sont premiers entre eux. En effet, si un nombre premier p divise a et b, il divise $a^2 + b^2$, c'est-à-dire c^2. On en déduit que p divise c, ce qui contredit le fait que a, b et c sont premiers entre eux. On montre de même que a et c sont premiers entre eux.

3) On remarque ensuite, en raisonnant par l'absurde, que l'un des nombres a ou b est pair. L'idée est de raisonner modulo 4, mais on peut écrire le raisonnement sans parler explicitement de classes modulo 4 : si a et b sont tous les deux impairs, il existe des entiers k et l tels que $a = 2k + 1$ et $b = 2l + 1$. On a donc $a^2 + b^2 = 4(k^2 + l^2 + k + l) + 2$. Il existe un entier m tel que $c = 2m$ ou $c = 2m + 1$, donc $c^2 = 4m^2$ ou $c^2 = 4(m^2 + m) + 1$: en

comparant les expressions de $a^2 + b^2$ et de c^2, on voit que 4 divise 2 ou 1, ce qui est impossible.

4) Comme a et b ne peuvent être tous les deux pairs d'après le 2), l'un est donc impair et l'autre est pair. On peut supposer que a est impair et que b est pair ; on pose $b = 2b'$, avec b' entier. Il est alors clair que c est impair, donc $c - a$ et $c + a$ sont des entiers pairs.

5) Posons $u = \dfrac{c-a}{2}$ et $v = \dfrac{c+a}{2}$. On vient de voir que u et v sont entiers. On a $u + v = c$ et $v - u = a$. Cela permet de montrer que u et v sont premiers entre eux. En effet, si un nombre premier p divise u et v, il divise leur somme c et leur différence a, ce qui implique que a et c ne sont pas premiers entre eux et contredit le 2).

6) On a $uv = b'^2$. Le théorème sur l'existence et l'unicité de la décomposition des entiers en produits de facteurs premiers montre que u et v sont des carrés.

7) Il existe donc des entiers m et n tels que $u = n^2$ et $v = m^2$, d'où les formules du théorème.

Aspect trigonométrique

Un des aspects remarquables de la tablette Plimpton 322 est de classer les couples donnés par les colonnes II et III suivant les valeurs décroissantes de c^2/b^2 (éventuellement diminué de 1). Tout se passe *comme si* les triangles correspondants aux différentes lignes étaient classés suivant la décroissance du plus petit angle aigu (alors que leurs côtés ont des valeurs très variées, plus ou moins grandes) à l'aide des chiffres de la colonne I. Cela ressemble-t-il à de la trigonométrie, 2000 ans avant Ptolémée ? Il ne faut sans doute pas analyser trop la tablette en fonction de ce qui s'est passé longtemps après son écriture, et noter aussi qu'aucune autre tablette de l'époque ne parlant d'angle, on ne peut supposer que celle-ci le fasse.

On peut calculer cette colonne (à 1 près) en effectuant des quotients suivis d'une élévation au carré puisque $\dfrac{c^2}{b^2} = \dfrac{1}{4}(\dfrac{m}{n} + \dfrac{n}{m})^2$ et $\dfrac{c^2}{b^2} - 1 = \dfrac{1}{4}(\dfrac{m}{n} - \dfrac{n}{m})^2$.

Nous avons dit que les bayloniens ne faisaient pas de division, mais utilisaient des tables d'inverses. Si la table leur donnait m' comme inverse de m et n' comme inverse de n, ils calculaient

$$\frac{m}{n} \pm \frac{n}{m}$$

en effectuant les multiplications mn' et $m'n$ et en faisant leur somme ou leur différence.

C'est peut-être la limitation de leurs tables d'inverses à des nombres comme 81 (l'inverse de 125 apparaît par ailleurs) qui explique qu'ils n'aient pas poussé leurs calculs plus loin.

Reconstruction de la tablette

Nous allons montrer dans ce paragraphe comment retrouver les triplets de la tablette à partir de quelques idées simples. Cela ne suppose pas que les idées du ou des inventeurs de la tablette aient été celles-là.

Voici les quatre critères que nous retenons, en suivant les idées de Neugebauer et Sachs.

1) Si m et n sont des entiers, avec $m > n$, le triangle de côtés a, b, c définis par $a = m^2 - n^2$, $b = 2mn$, $c = m^2 + n^2$ est un triangle rectangle.

2) Les côtés du triangle rectangle ainsi formé ne sont pas toujours premiers entre eux, mais on évitera de rencontrer ce cas trop souvent en choisissant m et n premiers entre eux ; si m et n sont tous les deux impairs, les trois nombres du triplet obtenus sont pairs.

3) Le quotient $\frac{c^2}{b^2} = \frac{1}{4}(\frac{m}{n} + \frac{n}{m})^2$ admet un développement fini en base 60 si m et n n'ont que 2, 3 et 5 comme facteurs premiers (on a dit qu'on appelait réguliers ces nombres) ; on se placera dans ce cas, en se limitant à $n = 54, m = 125$.

4) Le plus petit angle α du triangle varie entre un peu plus de 31° et 45°.

On obtient alors les seules possibilités suivantes [2].

2. Pour une étude détaillée de la tablette, on peut consulter **[FMPH-VI]** : *Faire des mathématiques à partir de leur histoire*, VI, IREM de Rennes.

n	m	a	b	c	α
1	2	3	4	5	36,87
4	9	65	72	97	42,08
5	9	56	90	106	31,89
5	12	119	120	169	44,76
8	15	161	240	289	33,86
9	20	319	360	481	41,54
12	25	481	600	769	38,72
15	32	799	960	1249	39,77
25	48	1679	2400	2929	34,98
25	54	2291	2700	3541	40,32
27	50	1771	2700	3229	33,26
27	64	3367	3456	4825	44,25
32	75	4601	4800	6649	43,79
40	81	4961	6480	8161	37,44
54	125	12709	13600	18541	43,27

La recherche des triplets avec $32° < \alpha < 45°$

3.4 Otto Neugebauer

Otto Neugebauer est né à Insbrück en 1899 et il est mort en 1990. Il étudie les mathématiques après la guerre à Göttingen qui est alors l'un des plus grands centres de recherche en mathématiques.

Il s'intéresse aux mathématiques anciennes, apprend l'égyptien et l'akkadien. À partir de 1927, il se consacre à l'étude des mathématiques babyloniennes dont il montrera dans de nombreuses études très soigneuses et qui font autorité, la richesse extraordinaire.

Simultanément, il codirige l'Institut mathématique de Göttingen avec Richard Courant. Göttingen était alors un des grands centres de recherche mathématique. Y travaillaient alors David Hilbert, vieillisant, Emmy Noether, une des rares femmes mathématiciennes de l'époque, etc.

Pour permettre aux mathématiciens de prendre connaissance des publications mathématiques de plus en plus nombreuses de leur temps dans un délai raisonnable, il a l'idée de publier un journal présentant des résumés de ces articles. Il convainc les éditions Springer-Verlag de le soutenir et le premier

numéro du *Zentralblatt für Mathematik* paraît sous sa direction en 1931. Ce journal s'impose rapidement.

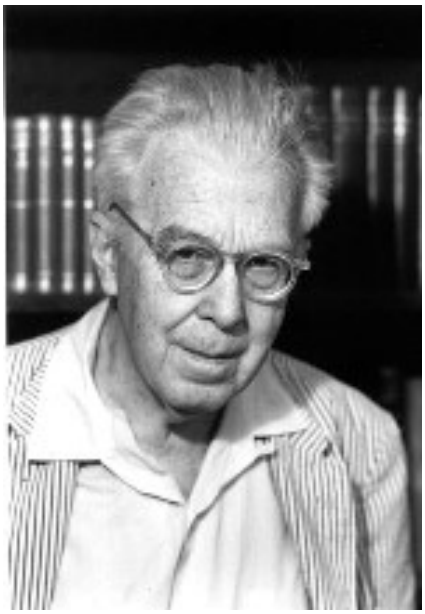


FIGURE 3.4 – Otto Neugebauer (Brown university).

Mais la montée du nazisme oblige Neugebauer, comme presque tous les mathématiciens de Göttingen, à quitter l'Allemagne. Il est d'abord invité à Copenhague par Harald Bohr (le frère de Niels Bohr) ; il a emporté avec lui sa documentation et peut continuer la publication du Zentralblatt. En 1938, la pression nazie est de plus en plus forte et Neugebauer et ses collaborateurs doivent abandonner le journal.

Neugebauer est alors invité aux Etats-Unis, à l'Université Brown. Il arrive avec les fichiers du Zentralblatt, ce qui lui permet, avec Tamarkin et Veblen, de fonder les *Mathematical reviews* en janvier 1940. Depuis cette date, cette revue est un élément essentiel de l'activité mathématique internationale et tous les mathématiciens la consultent régulièrement (tout à fait hors de notre sujet, notons que la revue permet une évaluation grossière du nombre de résultats mathématiques publiés chaque année : 3 résultats par article analysé, 7 articles analysés par page, 400 pages par numéro, 12 numéros par an donnent 100800 résultats, sans compter les résultats non analysés par la revue, non publiés ou tenus secrets pour raison militaire ou économique).

Neugebauer a ensuite continué à s'intéresser aux mathématiques de l'Antiquité, publiant une œuvre considérable, par exemple ses trois volumes sur l'histoire de l'astronomie de l'Antiquité.

On peut regretter que Neugebauer ait brûlé sa correspondance avant sa mort, ce qui nous prive d'une documentation de première main sur l'histoire des domaines qu'il avait étudiés pendant 70 ans.

Chapitre 4

Mesure de la Terre

Ce chapitre s'appuie en partie sur des travaux réalisés avec un groupe IREM, en particulier un article de Pascal Quinton [1] dont je reprends des passages. Le thème de la mesure de la Terre peut donner lieu à diverses activités mathématiques dans les classes de lycée, permettant d'illustrer diverses notions figurant au programme de ces classes et donnant l'occasion d'une réflexion scientifique approfondie. L'histoire de la mesure de la Terre est extrêmement riche depuis plus de 2000 ans ; nous n'en pouvons donner que quelques épisodes.

4.1 La Terre est ronde

Imaginons nos ancêtres se promenant dans la campagne, au bord de la mer, au sommet d'une montagne. Celui d'entre eux qui auraient proclamé que la terre est sphérique serait certainement passé pour un fou. L'idée que la terre est ronde semble être née chez des Grecs des années -500 (école de Pythagore) et non de Galilée (il s'agit dans ce cas du mouvement de la Terre autour du Soleil). Un siècle auparavant, des gens comme Thalès pensaient la Terre plate.

Ptolémée est l'un des plus grands savants de l'Antiquité. Il vivait à Alexandrie dans les années 100-150 d'après les phénomènes astronomiques qu'il dit avoir observés. La traduction en arabe de sa *Syntaxe mathématique*, sous le nom d'*Almageste* a eu une influence considérable sur la science arabe et

1. Voir *Actes du 13^{Øme} congrès Inter-IREM d'Histoire des mathématiques*, Rennes, 2000.

médiévale. Voici comment il discute de la forme de la Terre [2].

Que la Terre aussi, quand elle considérée dans son ensemble, soit sensiblement en forme de sphère, voici comment on pourrait le concevoir : le Soleil, la Lune et les autres astres, on peut le constater, ne se lèvent pas (ou ne se couchent pas) au même instant pour tous les hommes sur Terre, mais ils le font toujours plus tôt pour ceux qui habitent vers l'orient, toujours plus tard pour ceux qui habitent à l'occident. En effet, nous découvrons que les observations d'éclipses, et tout particulièrement celles de la Lune, qui sont pourtant faites au même instant, ne sont pas rapportées partout à la même heure (c'est-à-dire à égale distance par rapport au midi), mais que les heures notées par les plus à l'est des observateurs sont toujours plus tardives que celles notées par les plus à l'ouest. Et puisque la différence des heures est trouvée proportionnelle à la distance entre les lieux, c'est à bon droit que l'on peut assumer que la surface de la terre est sphérique, parce que sa surface arrondie d'une manière homogène (lorsqu'elle est prise comme un tout) masque [des parties du ciel] pour [les observateurs] successifs d'une manière proportionnelle. Or, si laTerre présentait quelque autre forme, cela n'arriverait pas, comme le montrent les considérations suivantes.

Si la Terre était concave, les astres en se levant apparaîtraient d'abord aux habitants les plus proches de la région du couchant ; si elle était plate, [les astres] se lèveraient et se coucheraient en même temps pour tous les habitants de la Terre ; si elle avait la forme d'un triangle ou d'un quadrilatère ou de quelque autre parmi les polygones, de nouveau [les astres se lèveraient et se coucheraient] de la même façon et au même instant pour ceux qui habitent sur la même surface plane : or on voit bien que cela ne se produit en aucune façon.

Que la Terre ne peut pas non plus être en forme de cylindre, de telle sorte que la surface incurvée soit tournée vers le levant et le couchant, tandis que les côtés plats qui forment les bases seraient dirigés vers les pôles de l'univers, comme certains pourraient l'accepter comme étant tout à fait plausible, voici qui le montre. Pour aucun des habitants de la surface incurvée, aucun des astres ne serait toujours visible, mais ou bien tous et se lèveraient et se coucheraient pour tous les hommes, ou bien les mêmes astres, distant d'une distance déterminée de chacun des deux pôles, seraient toujours invisibles pour tous les hommes. Or dans la réalité, plus nous nous avançons vers le

2. Traduction de A. Segonds et J.-P. Verdet. Textes essentiels. Astronomie et Astrophysique

nord, plus nombreuses parmi les étoiles du sud sont celles qui deviennent cachées, plus nombreuses au contraire parmi les étoiles du nord celles qui apparaissent ; cela montre donc clairement que la courbure de la terre, cachant régulièrement les astres dans la direction nord-sud dans tous les cas, établit que la forme [de la Terre] est de type sphérique.

À cela s'ajoute encore le fait suivant : si nous faisons voile vers des montagnes ou quelque endroit élevé, depuis quelque direction que ce soit, nous voyons leur grandeur s'accroître petit à petit, comme s'ils surgissaient de la mer elle-même, alors qu'auparavant ils y étaient plongés comme à cause de la courbure de la surface de l'eau.

Je laisse aux lecteurs et lectrices le soin de se convaincre par des dessins des différents arguments de Ptolémée.

Il ne faut pas oublier ce qui se passe à la période médiévale : on oublie les connaissances de l'Antiquité, on ne lit plus les textes grecs anciens ; les élites cultivées (Saint Augustin, Isidore de Séville, etc.) conçoivent de nouveau la Terre plate comme l'indique la Bible ; elle a la forme d'un disque et son centre est Jérusalem.

4.2 Mesure de la circonférence terrestre par Ératosthène

Une autre idée vraiment extraordinaire est de penser que, puisque la Terre est ronde, on pourrait la mesurer. Son étendue autour de nous semble un obstacle insurmontable. Cependant, la solution d'Ératosthène est extrêmement simple.

Ératosthène a vécu à Alexandrie, en Égypte, de 273 à 192 avant Jésus-Christ. On lui doit en particulier la méthode de recherche des nombres premiers à l'aide de son fameux crible.

Voici comment Jean-Étienne Montucla (1725-1799) raconte, dans sa monumentale *Histoire des mathématiques*, publiée à partir de 1758, la vie d' Ératosthène :

Ératosthène fut un de ces hommes rares dont le génie étendu embrasse tous les genres de savoir : orateur, poète, antiquaire, mathématicien et philosophe... Ce vaste savoir le fit choisir par le troisième Ptolémée pour son bibliothécaire, emploi qu'il exerça jusqu'à l'âge de quatre vingt ans, où, las d'une vie infirme et languissante, il la termina en se laissant mourir de faim.

Il eût été plus philosophique d'attendre la mort de pied ferme.

Philosophique ? C'est Montucla qui le dit.

Montucla décrit ensuite la manière dont Ératosthène a effectué sa mesure ; Syène est le nom grec d'Assouan (là où Nasser fit construire le second barrage d'Assouan, l'un des plus grands du monde, il y a 50 ans).

Il y avoit à Syène, un puits profond qui étoit entièrement illuminé à midi, le jour même du solstice d'été. Ératosthène l'avoit remarqué ; et comme à 300 stades à la ronde les hauteurs verticales ne jettoient pas d'ombre à ce moment, il en concluoit que Syène étoit précisément sous le tropique du Cancer. Il supposoit ensuite que Syène et Alexandrie étoient l'une et l'autre sous le même méridien et il estima leur distance de 5000 stades. Il ne s'agissoit plus que de connoître quelle partie du méridien terrestre étoit l'arc compris entre ces deux villes. Pour y parvenir, il attendit à Alexandrie le midi du jour du solstice, moment où le soleil étoit absolument vertical à Syène ; et (...) il mesura l'arc intercepté entre le soleil alors au zénith de Syène et le zénith d'Alexandrie. Il le trouva par-là d'une 50-ème partie de la circonférence, d'où il conclut que la grandeur du degré terrestre étoit de 250 000 stades.

On peut schématiser ainsi la situation. On a représenté le méridien passant par Alexandrie (point A) et Syène (point B). Ce méridien est un cercle dont le centre O est le centre de la terre.

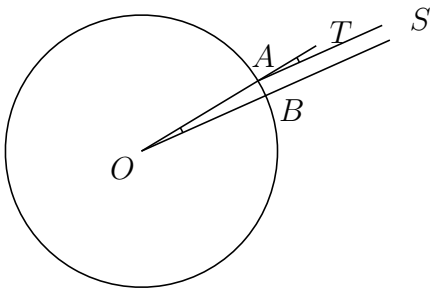


FIGURE 4.1 – La mesure d'Ératosthène.

Les droites (OAT) et (OBS) sont les verticales d'Alexandrie et de Syène, les rayons (SA) et (SB) sont parallèles, donc l'angle $\widehat{AOB}$ est égal à l'angle $\widehat{SAT}$. Ératosthène donne la valeur de ce dernier angle : 7°12, soit exactement 360°/50. Comme il sait que la distance de Syène à Alexandrie est de 5 000 stades, la circonférence de la terre est de $50 \times 5\ 000 = 250\ 000$ stades. La valeur finale d'Ératosthène est 252 000 stades pour avoir un nombre entier de

stades par 60-ième de circonférence : 4 200 stades (la division du cercle en 360 parties s'impose un siècle plus tard). On voit bien qu'Ératosthène a arrondit les distances et les angles, a supposé la concordance exacte des méridens de Syène et Alexandrie. Le problème principal est qu'aucun document ne permet de préciser la valeur du stade : on peut hésiter entre des valeurs très différentes, donnant pour le tour de la terre entre 24000 km et 46000 km, ce qui serait malgré tout de beaux résultats.

La figure que nous avons tracée suppose de savoir que la terre est ronde et que le soleil est comme à l'infini. George Gamow (1904-1964), un brillant cosmologiste, expliquait, dans un de ses livres de vulgarisation, *Une étoile nommée soleil*, apparemment sérieusement, qu'Anaxagore (-500 à -428) ayant déjà les données précédentes, mais supposant la terre plate et le soleil à distance finie, voyait le triangle SAB rectangle en B et, trouvant $\widehat{SAT} = 7°12$, en déduisait $\widehat{SAB} = 82°48$, puis $SB \approx 6500$ km. Cela a tellement l'air de la vérité que l'histoire est maintenant donnée comme vraie par des programmes et des manuels de physique français !

Signalons enfin que la mesure de la Terre retenue au Moyen-ge était plus petite que la mesure d'Ératosthène, seulement 180 000 stades. Certains supposent que Christophe Colomb, connaissant la distance de l'Extrême Orient par les routes de l'est, a pu en déduire qu'il n'était pas si loin que ça par l'ouest et lancer ses Caravelle vers l'ouest. Il est mort persuadé d'avoir réussi.

4.3 Débuts de la triangulation

Il y eut quelques tentatives de renouveler la mesure d'Ératosthène, trop approximatives pour l'égaler. Il fallait une nouvelle idée. Elle viendra de ce qu'on appelle la résolution des triangles. Connaissant quelques éléments d'un triangle (trois côtés, deux côtés et un angle, etc.) on peut calculer tous les éléments du triangle à l'aide de quelques formules de trigonométrie [3]. En plaçant une chaîne de triangles entre deux points et en mesurant des éléments de chacun des triangles, on parvient à déterminer la distance des deux points. Cette idée va se préciser au seizième siècle.

L'avantage de la méthode de triangulation est qu'elle ne nécessite qu'une mesure de distance au sol. Les autres mesure sont des mesures d'angles ; au

3. On trouve une illustration de cette méthode dans un texte d'Alberti (1404-1472) ; il s'agit de distances entre des tours proches formant un seul triangle.

fil des siècles, ces dernières mesures vont être de plus en plus précises.

Gemma Frisius

C'est Reynier Gemma Frisius (de la Frise, province hollandaise, 1508-1555), , médecin, mathématicien et astronome à Louvain, qui présente en 1533, dans un appendice de 16 pages à la *Cosmographie* de Apian, l'idée de la mesure d'une distance entre villes sous une forme nouvelle : à partir d'une distance connue mesurée au sol. Gemma suppose connaître la distance de

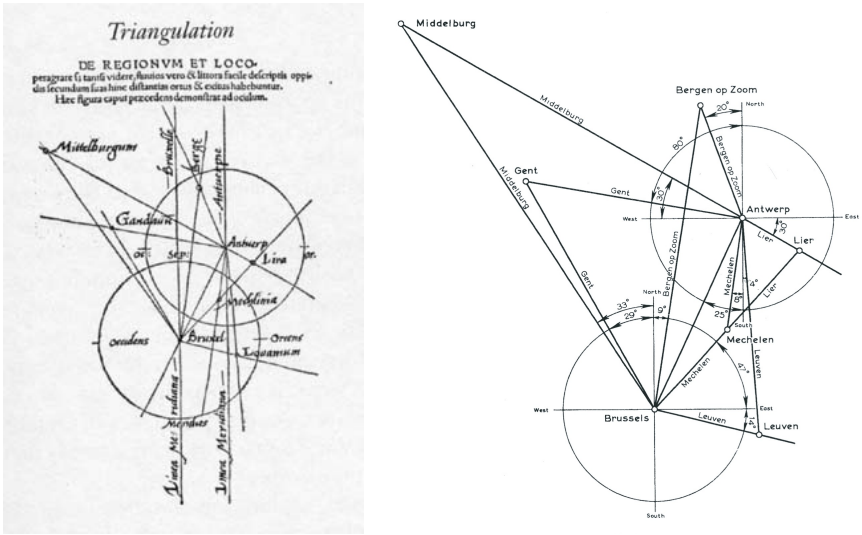


FIGURE 4.2 – La triangulation de Gemma Frisius.

Bruxelles à Anvers et montre comment en déduire par de simples mesures d'angles, les distances d'autres villes de ce qui n'était pas encore la Belgique ; il s'agit de mesures sur plusieurs triangles ayant la même base ; Gemma n'explicite pas les formules intentionnellement : elles sont trop difficiles pour le commun des mortels, écrit-il (en fait, il n'en donne aucune). Il précise que son schéma est théorique puisqu'il a choisi des villes qui sont trop éloignées pour être visibles l'une de l'autre et que la mesure de la distance de Bruxelles à Anvers est irréalisable. Pour la mesure des angles, l'appareil de Gemma est une sorte de goniomètre rudimentaire et les mesures sont au degré près ; la figure de Gemma montre qu'il ne faut pas se contenter de mesurer l'angle

qu'on cherche, mais mesurer également les autres angles d'un tour complet. Dans son exemple, Gemma ne donne pas de chaînes de triangles.

Gemma met en garde contre une utilisation de sa méthode sur de trop longues distances, car il est impossible d'appliquer la sphère sur le plan sans déformations. Un des élèves de Gemma est Gerardus Kremer dit Mercator (1512-1594) célèbre pour son ensemble de cartes des différentes parties de la Terre, utiles aux marins de son époque, avec la projection qui porte son nom ; les cartes de Mercator sont assez fidèles à la réalité pour les côtes européennes. Pour les côtes des îles de l'extrême orient, l'Australie et surtout l'Antarctique, c'est encore très fantaisiste.

FIGURE 4.3 – Mercator : cartes des deux hémisphères.

Jean Fernel

Une mesure du méridien sans triangulation est vraiment originale. Elle est due à Jean Fernel (1497-1558) qui fut un grand médecin. Picard raconte. *Fernel, au commencement de sa Cosmothéorie*[4]*, dit qu'étant parti de Paris, il marcha directement vers le nord, jusqu'à ce que, par les hauteurs méridiennes*

4. Ioannis Fernelii Ambianatis Cosmotheoria, libros duos complexa, Parisiis, in aedibus Simonis Colinaei, 1527.

du Soleil, il eût trouvé la hauteur du Pôle plus grande qu'à Paris d'un Degré entier : mais... il nous a célé le lieu où il s'est arrêté, disant seulement que c'étaiit à vingt-cinq lieues de Paris, & que pour sçavoir plus précisément cette distance, il monta dans un coche, compta tous les tours de rouë jusqu'à Paris ; & qu'enfin ayant estimé ce que les inégalités & les détours des chemins avoient pû apporter d'augmentation, il jugea qu'un Degré d'un grand cercle de la Terre contenoit 68 096 pas géométriques, qui selon notre façon de mesurer, valent 56 746 toises 4 pieds de Paris.

Avec une méthode aussi grossière, la précision du résultat de Fernel est assez incroyable : 39 816 kilomètres ; la part du hasard...

Tycho Brahé

Tycho (Tyge) Brahé (1546-1601), le grand astronome danois, est connu pour avoir fait des observations d'une grande précision en construisant ses propres instruments, d'autant plus remarquables qu'elles étaient faites à l'œil nu, les lunettes n'étaient pas encore inventées. Le roi du Danemark lui avait permis de construire un observatoire sur l'île de Hven entre le Danemark et la Suède, à Uraniborg. La triangulation entreprise autour de son île par Tycho Brahé est constituée de 11 villes (Copenhague, Helsingor, Hälsinborg, etc.) formant des triangles ayant presque tous la même base, très courte, allant de son observatoire à l'église de Hvenl. Les triangles peuvent avoir un angle au sommet de 4 degrés, ce qui induit des erreurs systématiques importantes, ses instruments ne lui permettaient qu'une précision de 4 minutes sur les angles.

C'est également Snel qui découvre la loi de réfraction des rayons lumineux passant d'un milieu dans un autre, loi qu'on attribuait à Descartes seul dans le temps.

Snel entreprend en 1616 une mesure du méridien terrestre. Le livre qu'il publie en 1617 a pour titre : *Eratosthenes Batavus De Terræ ambitus vera quantitate* ; c'est à juste titre que Snel peut se dire Ératosthène batave : il mesure une longueur de méridien au sol et détermine les latitudes des deux villes hollandaises : Alkmaar au nord et Berg op Zoom au sud ; sa grande originalité est d'avoir mesuré sa distance au sol par triangulation ; son gros défaut est d'être parti d'une base très courte (un peu plus de 300 mètres). Snel est le premier à définir soigneusement son unité de mesure, le rijnlandse roede, la perche ou verge du Rhin, mais elle ne nous est pas parvenue précisément (environ deux toises : 3,767 mètres) ; les mesures de l'époque variaient d'une région à l'autre. Snel conduit ses calculs avec des nombres décimaux, intro-

duits par Simon Stevin. Après bien des calculs et quelques petites erreurs, sans tables de logarithmes, Snel obtiendra une mesure de la circonférence terrestre de 38500 kilomètres ; avec tout le soin qu'il y avait mis, Snel avait une marge d'erreur bien plus faible qu'Ératosthène.

Snel van Royen

Willebrord Snel van Royen (1580-1626) est aussi connu sous son nom latin de Snellius. Il est né près de Gouda, en Hollande ; son père devient professeur de mathématiques à l'Université de Leide ; Snel commence à donner des cours de mathématiques dans cette université à 19 ans. Il rencontre Tycho Brahé à Prague en 1600, sans qu'on sache s'ils ont échangé des idées sur la triangulation. Il se marie en 1608 ; de ses 18 enfants, seuls trois lui survivront.

Willebrord Snel van Royen (1580-1626) est connu pour avoir énoncé la loi de réfraction de la lumière en 1621, une quinzaine d'années avant Descartes. Il n'est pas cité par Descartes, mais il faut dire qu'il n'avait pas publié sa découverte.

Snel publie sa mesure du méridien en 1617 sous le titre ambitieux et exact *Eratosthenes Batavus*[5]. La mesure de Snel souffre des mêmes défauts que celle de Tycho-Brahé : s'il mesure cinq bases au sol (faciles à réaliser : le sol de la Hollande est plat !), elles sont très courtes, quelques centaines de mètres, ce qui affecte la précision du résultat. Mais Snel va beaucoup plus loin que ses prédécesseurs : il situe les unes par rapport aux autres les villes de Hollande du nord au sud et il en déduit la longueur du méridien, environ 28500 perches du Rhin, soit 55021 toises, ce qui donne 38 612 kilométres de longueur au méridien[6].

La méthode de Snel pour déterminer avec précision la longueur du méridien sera la base des mesures des siècles suivants.

Le principe de la méthode de triangulation pour la mesure du méridien

L'idée de la mesure est la même qu'au temps d'Ératosthène : mesurer un arc de méridien le plus précisément possible, en se tournant vers les étoiles

5. De Batave, nom de la tribu germanique qui a peuplé la Hollande

6. Pour plus de détails sur les mesures de Gemma, Tycho Brahé et Snel, voir le livre de N. D. Haasbroek : *Gemma Frisius, Tycho-Brahé and Snellius and their triangulations*, 1968.

FIGURE 4.4 – Les triangles de Snel.

pour connaître les latitudes, mais en utilisant une méthode de triangulation pour les mesures au sol. Tout les calculs peuvent être basés sur une simple

formule de trigonométrie : dans un triangle ABC, le rapport du sinus d'un angle au côté opposé est constant :

$$\frac{a}{\sin A} = \frac{b}{\sin B} = \frac{c}{\sin C}.$$

Cette formule se prête bien aux calculs avec des tables de logarithmes, puisque ceux-ci transforment les quotients en différences.

Une conséquence de cette formule est que si on connaît les angles de triangles formant une chaîne (au sens que deux triangles successifs de la chaîne ont un côté commun) reliant deux points A et Z, il suffit d'avoir mesuré un côté, comme BC (appelé la base de la mesure), pour en déduire de proche en proche tous les autres et déterminer alors la distance AZ', où Z' est la projection de Z sur le méridien de A. Le point Z' n'a pas besoin d'être matérialisé sur le terrain. Pour ne pas prendre trop de place, j'ai dessiné horizontalement le méridien.

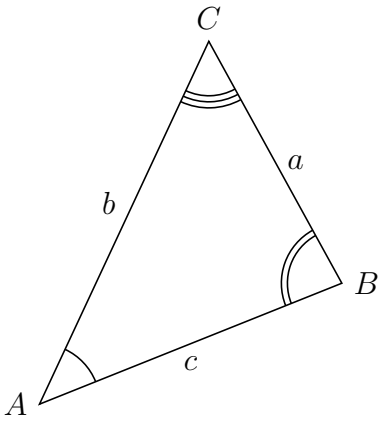


FIGURE 4.5 – Angles et côtés d'un triangle.

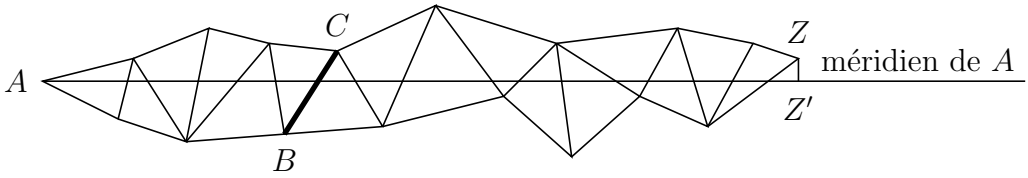


Figure 41

Si on note α (en degrés) la latitude de A et ζ celle de Z, et si on note d la distance AZ, la longueur du méridien terrestre est :

$$\frac{360}{\alpha - \beta} \times d.$$

4.4 Galileo Galilei (1564-1642)

Son prénom est Galilei, son nom Galileo, son père, Vincenzo (1520-1590) est un musicien connu.

Galilée est connu pour ses expériences sur la chute des corps et pour en avoir énoncé la loi. Il est connu pour sa condamnation (le 22 juin 1633), pour avoir osé affirmé son soutien au système de Copernic dans lequel la Terre perd sa place centrale au profit du Soleil. On sait qu'il fut assigné à résidence jusqu'à la fin de sa vie. C'est alors qu'il écrit *Discours concernant deux sciences nouvelles*, jetant les bases de la mécanique rationnelle. C'est là que, pour établir les lois du mouvement uniformément accéléré, il reprend les

méthodes d'Archimède, déduisant une égalité d'aires de l'égalité de segments se correspondant, restant aux portes du calcul intégral.

Une citation de Galilée est célèbre, à la fois parce qu'elle fait plaisir à l'ego des mathématiciens et surtout parce qu'elle annonce d'une façon visionnaire la naissance de la démarche scientifique moderne :

La philosophie est écrite dans cet immense livre qui se tient toujours ouvert devant nos yeux, je veux dire l'univers, mais on ne peut le comprendre si l'on ne s'applique d'abord à en comprendre la langue et à connaître les caractères avec lesquels il a été écrit. Il est écrit dans la 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. (*Il Saggiatore*, L'Essayeur,1623).

Dans ce chapitre, Galilée nous intéresse par ses travaux de 1609-1610.

En mars 1610, Galilée publie le *Siderus Nuncius*, le *Messager céleste*. Il y raconte comment il a obtenu en quelques semaines *des observations infiniment stupéfiantes* et nous allons voir qu'il a absolument raison.

En mai 1609, il a entendu parler de lunettes astronomiques construites depuis peu par des Hollandais ; il en fabrique lui-même une grossissant 30 fois et pense tout de suite à l'utiliser pour étudier le ciel la nuit.

Il la dirige vers la lune : une partie est éclairée par le soleil, l'autre pas ; la ligne de séparation ne lui apparaît pas régulière et il y a de petites zones éclairées dans la zone sombre. Galilée comprend que le phénomène est ana-

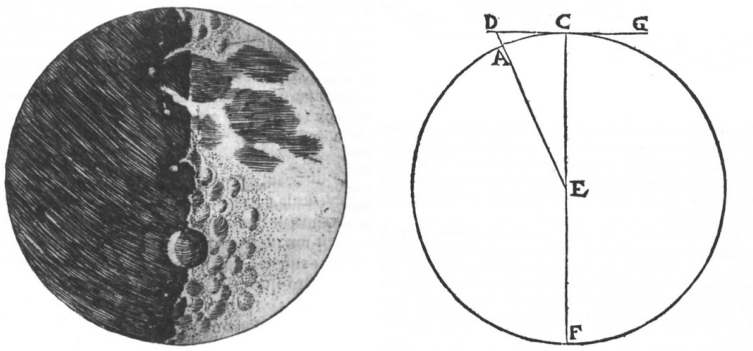


FIGURE 4.6 – Galilée, dessins de la lune et calcul de la hauteur des montagnes, décembre 1609.

logue à celui du soleil éclairant au couchant les sommets entourant une vallée

déjà plongée dans l'obscurité. Galilée connaît des estimations du diamètre de la Terre et, par conséquent, du diamètre de la Lune. Il en déduit (voir la figure 4.6) la hauteur d'une montagne lunaire : 4,987 miles, soit 7371 mètres, résultat remarquable de précision que Galilée accompagne d'un commentaire étonnant pour nous : *sur la terre, il n'existe pas de montagnes d'un seul mille à la verticale* ; on a donc connu la hauteur des montagnes de la lune, avant de connaître celle des montagnes des Alpes !

Puis Galilée découvre que la voix lactée est un *troupeaux* d'étoiles :

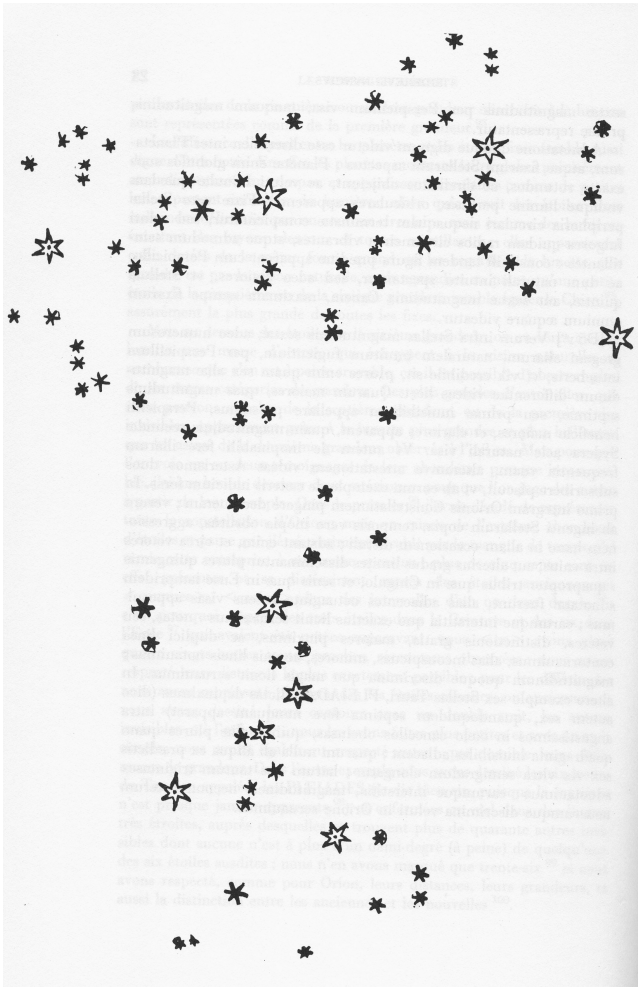


FIGURE 4.7 – Galilée, la voie lactée, décembre 1609.

Enfin, encore plus extraordinaire : *le 7 janvier 1610, à une heure de la nuit, comme j'observais le ciel à la lunette, Jupiter se présenta et ... je reconnus que trois petites étoiles, assurément menues, mais très brillantes, étaient près de lui.*

FIGURE 4.8 – Galilée, Jupiter la nuit du 7 janvier 1610.

Il les observe le 8 janvier : ce n'est plus la même disposition !

FIGURE 4.9 – Galilée, Jupiter la nuit du 8 janvier 1610.

Est-ce simplement parce que Jupiter a bougé ou y a-t-il autre chose ? Galilée attend impatiemment la nuit suivante : c'est nuageux et il ne peut rien voir. Enfin, le 10, il voit que les points brillants accompagnent toujours Jupiter.

FIGURE 4.10 – Galilée, Jupiter la nuit du 10 janvier 1610.

il les observe nuit après nuit : il est en train de découvrir les satellites de Jupiter : Ainsi la Terre n'était pas la seule planète du système solaire à avoir un satellite ! Découverte immense pour l'époque et que Galilée s'empresse de publier.

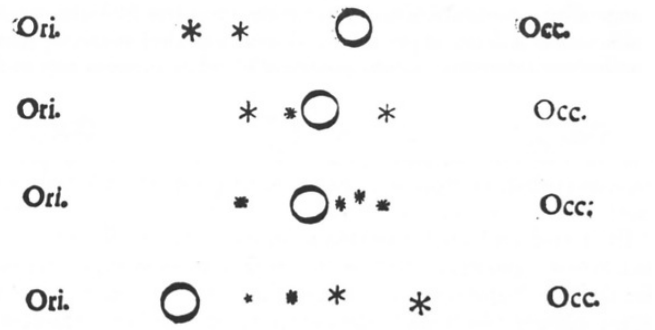


FIGURE 4.11 – Galilée, Jupiter les nuits du 11 au 14 janvier 1610.

4.5 La vie scientifique en France au XVII^{Øme} siècle

Autour de 1600

La première moitié du XVI^{Øme} siècle voit la contestation violente de l'Eglise romaine. Un des aspects de la contre-attaque de celle-ci est le développement de l'ordre des Jésuites par Ignace de Loyola (1491-1556) qui le créa en 1540. L'ordre cherche à former un homme nouveau, catholique romain ; la construction d'un réseau dense de collèges dans toute l'Europe avec partout le même type d'enseignement de qualité est essentiel dans sa stratégie. Le collège de La Flèche ouvre le 2 novembre 1603, celui de Rennes l'année suivante ; l'église du collège de Rennes sera construite quelques années plus tard : c'est l'actuelle église Toussaints, adossé au Lycée Émile Zola construit il y a un peu plus d'un siècle sur l'emplacement du collège. Je rappelle qu'un des tout premiers passages des *Mémoires d'Outre-tombe* est le récit, par Chateaubriand, de son passage au collège de Rennes et des combats (au compas !) dans les jardins du Thabor.

Les mathématiques sont une part substantielle de cet enseignement dans les petites classes ; dans les classes supérieures, elles ont leur place à côté de la philosophie et de la théologie. Ce sont les *Éléments* d'Euclide, dans une version pleine de commentaires variés due à Clavius (Christophe Schlüssel, dit Christophorus Clavius, 1537-1612) ou les *Éléments de géométrie* du père Tacquet (André Tacquet, 1612-1660) qui sont à la base de l'enseignement et non

les résultats récents des algébristes italiens (plus tard, les idées cartésiennes mettront un siècle à pénétrer dans les collèges !). Clavius, professeur pendant une trentaine d'années au collège de Rome insiste auprès de ses collègues sur la valeur des mathématiques favorisant la compréhension de la philosophie et la pratique des autres sciences et il souligne la certitude de leurs raisonnements.

En France, la période des guerres de religion ne favorise pas les études scientifiques. Le Collège de France a été créé par François 1er en 1530. Pierre de la Ramée dit Ramus (1512-1572) y enseigne la grammaire et la rhétorique ; il y introduit un cours de mathématiques en 1559 ou 1560 ; calviniste, il est assassiné deux jours après la Saint Barthélémy.

Le grand mathématicien de l'époque est François Viète dont nous reparlerons ; il travaille presque toujours isolé. A la fin de sa vie, il se lie d'amitié avec le belge Adriaan van Roomen et l'invite chez lui en Poitou. Il diffuse les tirages, très faibles, de ses œuvres auprès de ses amis. Sous le règne d'Henri IV, la pacification du royaume, le développement d'une vie économique, favorisent sans doute l'éclosion d'une vie intellectuelle et, en particulier, scientifique, centrée à P aris.

Autour de Mersenne

C'est l'occasion de parler d'un homme attachant, s'intéressant à tout, d'une activité incessante. Le livre de Beaulieu [7] donne beaucoup de détails sur lui ; nous décrirons son activité d'organisateur plutôt que ses propres travaux.

Marin Mersenne naît à Oizé, à 24 km du Mans, le 8 septembre 1588. Sa famille est aisée. Il se souviendra plus tard du plaisir de voir battre le blé et critiquera les sorcières soufflant sur l'herpès ou récitant des pater ; on sait que des pratiques de sorcellerie ont toujours cours dans ces régions et sans doute dans bien d'autres.

Il étudie le latin et le grec au collège du Mans à 12 ans puis au collège de La Flèche nouvellement ouvert par les jésuites où il entre en contact avec les disciplines scientifiques . Il poursuit ses études à Paris en 1605 et entre dans l'ordre des minimes, recevant l'habit le 16 juillet 1611. Il part enseigner la philosophie et la théologie à des religieux de son ordre à Nevers.

7. Beaulieu Armand : Mersenne le grand minime.— Bruxelles : Fondation Nicolas-Claude Fabri de Peiresc, 1995.— 379 p.

Il débute une amitié avec Nicolas Peiresc, aristocrate provençal féru de sciences. Celui-ci avait observé en 1610, avec une lunette fabriquée à Paris (les premières lunettes datent de 1608), les satellites de Jupiter découverts au début de l'année par Galilée et pensera, le premier peut-être, à les utiliser pour déterminer la longitude d'un lieu. Leur correspondance, qui traite de nombreux sujets scientifiques, ne cessera qu'à la mort de Peiresc en 1637.

Mersenne a vraiment de bons côtés ; il écrit : *Il n'y a point de sciences, après la théologie, qui nous proposent et nous fassent voir tant de merveilles comme font les mathématiques, lesquelles élèvent l'esprit par dessus soi-même et le forcent à reconnaître une divinité*

Mersenne se pose beaucoup de questions ; Pascal indique, dans son histoire de la roulette : *Le feu père Mersenne, Minime, fut le premier qui la remarqua environ l'an 1615, en considérant le roulement des roues, ce fut pourquoi il l'appela La Roulette. Il voulut ensuite en reconnaître la nature et les propriétés, mais il n'y put pénétrer.* Pascal ajoute, ce qui va donner une idée de l'importance de Mersenne : *Il avait un talent tout particulier pour former de belles questions ; en quoi il n'avait peut-être pas de semblable : mais encore qu'il n'eût pas un pareil bonheur à les résoudre, et que ce soit proprement en ceci que consiste tout l'honneur, il est vrai néanmoins qu'on lui a obligation, et qu'il a donné l'occasion de plusieurs belles découvertes, qui peut-être n'auraient jamais été faites s'il n'y eût excité les savants.*

Il revient à Paris en 1619. La place royale, future place des Vosges, se construit ainsi que, tout proche, le couvent des minimes, où va vivre Mersenne, et son église où Anne d'Autriche (1601-1666) vient prier les vendredis pour la fin de sa stérilité (elle a été mariée à Louis XIII (1601-1643) en 1615 et celui-ci attendra 23 ans avant de faire ce qu'il faut... ; plus tard sans doute, elle aura une liaison avec Mazarin). Mersenne a publié de très nombreux livres, le premier en 1623, contre les alchimistes. C'est un lecteur acharné, doué d'une mémoire extraordinaire et ne se laissant pas enfermer dans les règles strictes de son ordre. Il fait la connaissance de Descartes dès 1622, puis celle de l'astronome Gassendi et de bien d'autres, commençant à animer la vie scientifique de son temps, posant par exemple à Descartes des dizaines de questions diverses : musicales, physiques (distance à laquelle on entend un son, poids du pendule dans le vide), mathématiques (la division d'un cercle en 27 parties, en 29 parties égales, comparaison de quantités infinies, problème de Pappus, duplication du cube), linguistiques (invention d'une langue universelle, besoin d'éducation des enfants pour parler), etc.

Trop sollicité à Paris, Descartes s'établit en Hollande en 1628. Mais il

reste lié à Paris par la correspondance de Mersenne : *J'avais cet avantage pendant la vie du bon Père Mersenne, que bien que je ne m'enquisse jamais d'aucune chose, je ne laissais pas d'être adverti soigneusement de tout ce qui se passait entre les doctes ; en sorte que s'il me faisait quelques fois des questions, il m'en payait fort libéralement les réponses en me donnant avis de toutes les expériences que lui ou d'autres avaient faites, de toutes les rares inventions qu'on avait trouvées ou cherchées, de tous les livres nouveaux qui étaient en quelque estime et enfin de toutes les controverses qui étaient entre les savants.* Inversement, Descartes tient Mersenne au courant de ses travaux et celui-ci ne manque pas de les communiquer à d'autres.

Au début des années 1630, le monde scientifique est secoué par l'affaire Galilée dont nous ne parlerons pas ici. Mersenne continue ses publications à un rythme soutenu (*Questions inouyes*, 1634, 180 p., *Harmonie universelle*, 1636, 1500 p. ! Etc.).

Pour les savants ou amateurs de sciences, c'est le moment de structurer leurs relations. L'idée d'académie remonte au moins à l'École de Platon, qui se réunissait dans les jardins de Monsieur Akademos à Athènes au IV$^{\text{Øme}}$ siècle avant J.-C. On ne peut décrire en détail son évolution en Italie où l'Académie dei Lincei, avec Galilée, développe les idées modernes de 1603 à 1630. En France, les réunions de différents cercles se multiplient telle cette compagnie d'amis férus de littérature et de théâtre, à l'origine, en 1634, à la demande de Richelieu, de l'Académie française.

Pour les sciences, Mersenne propose dans ses Questions inouyes un programme général parlant : *de grands esprits, qui sont capables d'augmenter les sciences, et peut-être de les reformer en beaucoup de choses, ce que l'on pourrait aisément exécuter, si l'un travaillait à une partie de la physique, de la Médecine, etc. et les autres à d'autres parties, et si l'on conférait ensemble des difficultés qui se présentent, tant à la spéculation des principes, qu'en la déduction des conclusions, et dans la pratique des expériences.* Le 23 mai 1635, la correspondance de Mersenne à Peiresc montre la réalisation de cette idée : il parle de *la plus noble académie du monde... elle est toute mathématique.* Des réunions se tiennent régulièrement, le jeudi le plus souvent et à son couvent. La liste de ceux qui y participent, régulièrement ou à l'occasion d'un voyage à Paris est longue : Gassendi, Étienne Pascal et son fils Blaise, tout jeune, Girard Desargues, Claude Mydorge, Gilles Personne de Roberval, Jean de Beaugrand, Pierre de Carcavy,... Les discussions portent sur les sujets du jour, sur les questions et les solutions envoyées par ceux qui ne sont pas à Paris. Chaque réunion suscite de nouvelles questions et les

participants diffusent souvent à leurs amis la teneur de ce qui s'y est dit. Ainsi, l'influence de cette *Academia Parisiensis* s'étend à l'Europe entière. Constantin Huygens (le père de Christian) dira, en 1644, que Mersenne est *l'entremetteur de tous les honnêtes gens.*

Par exemple, en 1637, Roberval reçoit une lettre de Fermat un lundi, la communique le jeudi suivant *à l'assemblée de nos mathématiciens qui étaient ce jour là chez M. de Montholon*, où elle est étudiée et admirée ; Étienne Pascal est chargée d'en fournir des copies pour tous ; enfin, on discute du problème de Pappus.

Le rôle de Blaise Pascal, âgé de 12 ans en 1635, est évoqué par sa sœur Gilberte dans La Vie de Monsieur Pascal :

il se trouvait régulièrement aux conférences qui se faisaient toutes les semaines où les plus habiles gens de Paris s'assemblaient pour porter leurs ouvrages et pour examiner ceux des autres. Mon frère tenait fort bien son rang tant pour l'examen que pour la production, car il était un de ceux qui y portaient le plus souvent des choses nouvelles. On voyait aussi fort souvent dans ces assemblées des propositions qui étaient envoyées d'Allemagne et d'autres pays étrangers et on prenait son avis sur tout et avec autant de soin que de pas un autre ; car il avait des lumières si vives qu'il est arrivé qu'il découvrait des fautes dont les autres ne s'étaient point aperçus.

C'est en 1636 que Mersenne entend parler de Pierre de Fermat par Carcavy. Il lui écrit, Fermat répond ; on connaît 37 lettres de Fermat à Mersenne. Par le jeu des lettres de l'un transmises à l'autre et réciproquement, celui-ci créé une *petite guerre* entre Descartes et Fermat sur les problèmes de maximum et minimum, de la lumière, etc. Fermat n'est probablement jamais venu à Paris.

On peut dresser une liste de 180 membres de l'académie de Mersenne, parmi lesquels une quarantaine de mathématiciens, et ceci sans compter les nombreux correspondants étrangers de Mersenne.

Au retour d'un voyage en Italie de 1644 à 1645, rempli de contacts parfois difficiles avec Torricelli, Cavalieri... Mersenne fait connaître en France les expériences sur le baromètre. C'est l'origine des célèbres et décisives expériences du Puy de Dôme sur le vide que propose Pascal et qui sont réalisées le 19 septembre 1648.

Mersenne n'aura pas connaissance de ces mesures. Il est mort le premier septembre, regretté de tous les savants de son époque, pour avoir bu, dit-on, trop d'eau fraîche avec Descartes par un chaud jour d'août.

Enfin, signalons pour les lecteurs mathématiciens que Mersenne a donné,

en 1644, une liste, un peu inexacte, de nombres premiers de la forme $2^n - 1$, avec $n \leqslant 257$. Les nombres premiers de cette forme sont maintenant appelés nombres de Mersenne et c'est parmi eux qu'on a trouvé les plus grands nombres premiers connus, actuellement 36, pour $n = 2, 3, 5, 7, 13, 17, 19, 31, \ldots$, les plus grands étant pour $n = 1\ 398\ 269$ (13-11-1996, Joël Armengaud), $n = 2\ 976\ 221$ (24-8-1997, Gordon Spence), $n = 3\ 021\ 377$ (27-1-98, Woltman, Kurowski, Charleson) ; le dernier record est $n = 43\ 112\ 609$, près de 13 millions de chiffres, trouvé le 23 août 2008. Et c'est encore Mersenne qui réussit à faire imprimer, en 1646, au terme de 10 ans d'efforts, à Amsterdam, une grande partie des Œuvres de Viète.

4.6 L'Académie royale des sciences

Quelques années après la mort de Mersenne, deux grandes académies voient le jour. En Italie, c'est l'académie del Cimento, tournée vers les démarches expérimentales, qui perfectionne les instruments de la physique (1657-1667). En Angleterre, c'est la Royal society of London qui est reconnue officiellement le 15 juillet 1662.

En France, les troubles de la Fronde désorganisent le milieu scientifique parisien. Le Pailleur jusqu'en 1654, puis Montmor de 1657 à juin 1664, continuent à recevoir des savants et un règlement des réunions est même rédigé. L'idée d'académie est forte : l'académie de peinture et sculpture est fondée en 1648, celle de danse en 1661, celle des inscriptions et médailles en 1663. Une nouvelle initiative dans le domaine scientifique est lancée par Thévenot dans le courant de l'année 1664, mais elle s'arrête faute de fonds suffisants. Des projets précis circulent, Auzout propose la construction d'un Observatoire, ce qui demande de l'argent et une *Compagnie des sciences et des Arts*. Le temps est venu et les projets se précisent ainsi que les interventions auprès de Colbert. Quelques mathématiciens sont nommés en mai et juin 1666 : Huygens, Auzout, Roberval, Carcavy, Frénicle, Picard, Buot. Jusqu'en novembre 1666, il est envisagé une académie regroupant littéraires et scientifiques. Mais devant sans doute pressentir les problèmes difficiles que créerait cette cohabitation, seule l'Académie des sciences est lancée le 22 décembre 1666 avec 21 membres scientifiques dont les sept mathématiciens cités.

Les réunions sont fixées aux mercredis et samedis. L'académie fonctionnera ainsi jusqu'aux premières modifications du règlement en 1699.

Le pouvoir royal tire prestige de cette création qui demande un finan-

cement important pour les pensions de ses membres et pour leurs travaux. L'industrie et le commerce français en tire avantage car nombre de travaux sont très pratiques et améliorent la qualité des marchandises françaises.

La plus grande gloire de l'Académie est alors le hollandais Christian Huygens. Fils de Constantin Huygens, il correspond tout jeune avec Mersenne et réfute la démonstration de la quadrature du cercle proposée par Grégoire de Saint-Vincent en 1648. C'est le plus grand physicien du milieu du siècle. Il travaille sur les longueurs d'ondes, la réfraction et la vitesse de la lumière, la force centrifuge et la force d'inertie. Il perfectionne les instruments d'optique et d'astronomie, découvre la rotation de Saturne et ses anneaux... C'est lui aussi qui développe le calcul des probabilités après l'échange de lettres fondateur entre Pascal et Fermat de l'été 1654. Mais ce grand scientifique doit quitter la France en 1685 à la révocation de l'Edit de Nantes, même s'il est peut-être athée et non protestant. Des centaines de milliers de français, coupables de ne pas pratiquer la religion officielle, doivent en faire autant, dans des conditions dramatiques.

Nous avons déjà croisé Roberval à l'époque de Mersenne. Il avait contribué aux progrès des calculs différentiel et intégral : définition des tangentes aux courbes, problème de la cycloïde... En 1669, il invente la balance qui porte son nom.

Colbert souhaitait une carte de France plus précise pour la bonne gestion du royaume. L'un des premiers grands travaux de l'Académie sera la mesure d'un degré de méridien terrestre par Picard, ce dont nous allons parler plus en détail. La bonne précision de ce travail a été rendue possible par l'invention du micromètre d'Auzout qui perfectionne les lunettes astronomiques.

4.7 La mesure de Picard

L'abbé Jean Picard (1620-1682) [8] est né à La Flèche [9]. Comme Mersenne et Descartes, il étudie au collège de sa ville, l'un des meilleurs de France à cette époque. Il va ensuite à Paris, assiste l'astronome Pierre Gassendi

8. L'une de mes références principales pour la suite de ce chapitre est : Le vallois J.-J., *Mesurer la Terre 300 ans de géodésie française De la toise du Châtelet au satellite*, Presses des ponts et chaussées, 1988.

9. Pour cette mesure, voir Pascal Quinton, Activités mathématiques à propos de la mesure de la terre, in *4000 ans d'histoire des mathématiques*, Actes du treizième colloque Inter-IREM, IREM de Rennes, 2000.

(1592-1655) dans les années 1645-1655, puis devient professeur au collège de France. Nous avons dit qu'il fait partie des premiers membres de l'Académie des Sciences en 1666. Il semble avoir été particulièrement remarquable dans la qualité des appareils qu'il mettait au point et la précision de ses mesures.

Colbert souhaitait une carte de France plus précise pour la bonne gestion du royaume. L'Académie des Sciences chage Picard d'un premier travail, préalable l'établissement de cartes détaillées, la mesure de la longueur du degré du méridien à la latitude de Paris. Les mesures de Picard seront exécutées au cours des années 1669-1670 pour, écrit Picard, *l'utilité de la Géographie en ce qui concerne les différences des Longitudes, mais particulièrement encore pour l'usage de Navigation, d'autant plus que jusqu'à présent, personne ne s'était avisé de se prévaloir du grand avantage qu'on pouvait tirer des Lunettes d'approche pour l'exécution de ce dessein...*

Picard a écrit un compte rendu détaillé de son travail. Il y donne un historique des mesures de la Terre avant la sienne ; nous avons déjà cité ce qu'il dit de Fernel.

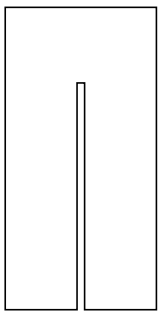
Le résultat et l'unité

Picard suppose encore la Terre sphérique. Son résultat est remarquable. Il obtient 57 060 toises pour un degré, soit 40 036 kilomètres. Mais il nous reste une incertitude concernant ce résultat, c'est celui de l'unité de longueur utilisée. Picard explique : *La toise... que nous avons choisie comme la mesure la plus certaine et la plus usitée en France, est celle du grand Châtelet de Paris, suivant l'original qui en a été nouvellement rétabli. Il s'agissait en fait d'une barre de métal encastrée dans un mur du grand Châtelet qui occupait la place du même nom actuelle. Cette barre était utilisée par tous ceux qui devaient vérifier leurs mesures à Paris, tapissiers, drapiers, etc. Quelques années plus tard, l'original avait été abîmé et il était impossible de déterminer avec précision sa longueur*

La rondeur de la Terre est moins altérée par les inégalités des montagnes, que celle de l'orange la plus fine par le grain de son écorce... explique Picard (les oranges étaient rares à son époque), justifiant le nécessaire recours à la géométrie pour mesurer une distance si considérable.

Le matériel

Le matériel de Picard est bien plus précis que celui de ceux qui l'ont précédé. Maupertuis en fait encore l'éloge en 1740. Picard explique que Snel a eu raison de rendre les pinnules responsables des erreurs de ses mesures : *au travers desquelles... un objet gros de plusieurs minutes n'était vu que comme un point, & encore avec peine.* Expliquons : l'alidade (mot d'origine arabe) est une règle portant à ses extrémités des pinnules, petites plaques fixées verticalement et comportant des fentes longitudinales de formes diverses. Les pinnules permettaient de diriger l'alidade dans une direction en alignant un objet éloigné avec les pinnules. L'alidade était fixée au centre d'un arc de cercle de plus ou moins grand rayon et gradué ; on pouvait donc connaître la direction de l'objet éloigné.



]

FIGURE 4.12 – Pinnule.

Comme la direction déterminée à l'aide des pinnules n'était pas connue avec une précision suffisante, Picard utilise un nouveau dispositif, dont *on s'est avisé depuis quelques années* : remplacer les pinnules par des lunettes d'approches, un dispositif qui le satisfait entièrement. La figure voir figure 4.13 reproduit l'appareil de Picard [10] ; le quart de cercle est ici placé verticalement ; on distingue, horizontale, la lunette dont parle Picard. Pour les mesures d'angles de la triangulation, l'appareil devait être parfaitement horizontal. *L'instrument a donné les angles avec tant de justesse, que sur le tour d'horizon pris en cinq ou six angles, on n'a jamais trouvé qu'environ une minute de plus ou de moins qu'il ne fallait, & que souvent aussi l'on a*

10. Dans sa grande entreprise de reproduction de textes anciens, Google présente en particulier le livre de PIcard ; si le texte est bien reproduit, les quatre planches sont décevantes : la photocopie les coupe de moitié.

approché du compte juste, à cinq secondes près.
On ne peut décrire toutes les précautions de Picard pour assurer la qualité

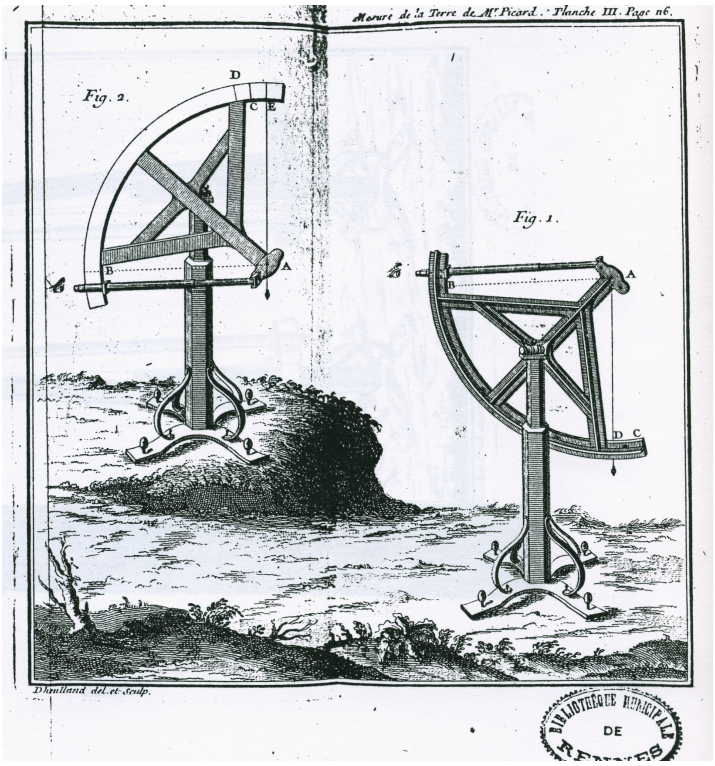


FIGURE 4.13 – L'appareil de Picard.

de son matériel et la précision de ses mesures. Il en parle longuement dans son texte ; notons juste, ce qui frappe le plus, l'installation d'un dispositif pour éviter que le vent ne perturbe le fil à plomb.

La chaîne de triangles

Dans le dessein que l'on s'était proposé de travailler à la mesure de la Terre, on a jugé que l'espace contenu entre Sourdon en Picardie, & Malvoisine dans les confins du Gâtinois et du Hurepoix, serait très commode pour l'exécution de cette entreprise ; car ces deux termes sont distants l'un de l'autre d'environ trente-deux lieues, sont situés à peu près dans un même

méridien, & l'on avait su par plusieurs courses faites exprès, qu'ils pouvaient être liés par des triangles, avec le grand chemin de vIllejuive à Juvisy, lequel chemin étant pavé en droite ligne sans aucune inégalité considérable... est propre pour servir de base fondamentale à toute la mesure...

Il y a 13 triangles principaux (voir figure 4.14) et quelques triangles supplémentaires ; les sommets $A, B, \ldots, Y$ sont des points choisis par Picard de telle façon qu'on puisse mesurer sans difficulté les angles des triangles ABC, ACD, etc. Ces points sont donc visibles de loin, et facilement identifiables. En voici la liste.

A est le milieu du moulin de Villejuive.

B le plus proche coin du pavillon de Juvisy.

C la pointe du clocher de Brie-Comte-Robert.

D le milieu de la tour de Monthléry.

E le haut du pavillon de Malvoisine.

F une pièce de bois dressée exprès au haut des ruines de la tour de Monjay, & grossie de paille.

G le milieu du Tertre de Mareuil, où l'on a été obligé de faire des feux pour le marquer.

H le milieu du gros Pavillon en ovale du Chaâteau de Dammartin.

I le Clocher de Saint Samson de Clermont.

L le clocher de Coivrel.

M un petit arbre sur la Montagne de Boulogne proche Montdidier.

N le Clocher de Sourdon.

O un petit arbre fourchu sur la Butte du Griffon, proche Villeneuve Saint Georges.

P le clocher de Montmartre.

Q le clocher de saint Christophe proche Senlis.

V le Clocher de Notre-Dame d'Amiens.

On peut retrouver la localisation de la plupart de ces points sur une carte actuelle.

La mesure de la base

La mesure de la base est un tour de force. Le *grand chemin de Villejuive*[11] *à Juvisy* est aujourd'hui un tronçon de 11 kilomètres de la nationale 7 ; il est en ligne droite, à l'exception d'un écart dû à l'aéroport d'Orly. Pour le mesurer, Picard fait tailler quatre poteaux de bois de deux toises chacun, les

11. Villejuif aujourd'hui.

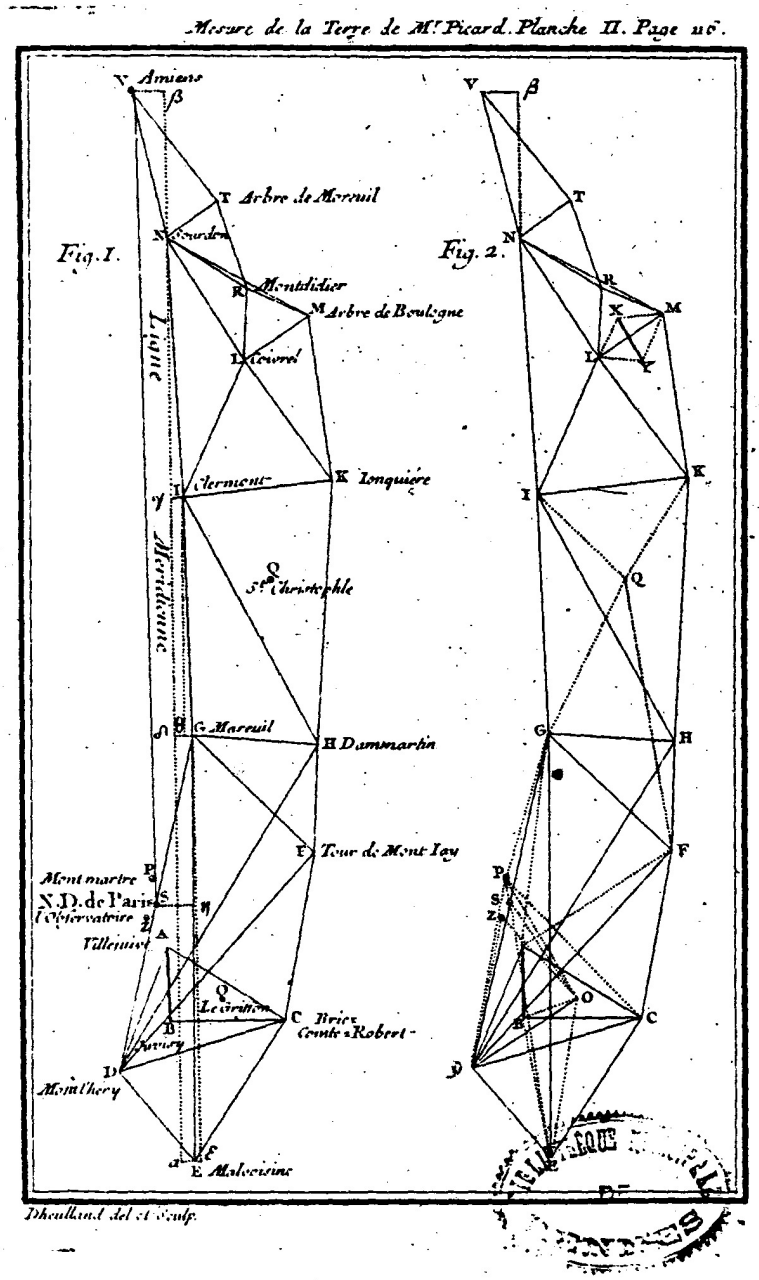


FIGURE 4.14 – Les triangles de Picard.

unit deux par deux pour faire des mesures de quatre toises. *L'ordre que l'on garda en mesurant, fut que lorsqu'une des mesures avoit été posée à terre, l'on y joignoit l'autre, bout à bout le long d'un grand cordeau ; puis on relevait la première, et ainsi de suite...* La mesure est faite deux fois ; Picard trouve 5662 toises cinq pieds en allant, 5663 toises un pied en revenant. Il prend la moyenne : 5663 toises, soit 11 kilomètres et 37 mètres 43.

Pour vérifier sa mesure, Picard mesurera une seconde base proche d'Amiens et de 3902 toises.

La détermination des triangles

En général, Picard mesure les trois angles de ses triangles et s'arrange quand la somme des trois angles ne fait pas exactement 360 degrés (il augmente par exemple de 10 secondes l'angle DFC). Parfois, il ne peut calculer l'un des trois angles, ne pouvant placer son quart de cercle dans les clochers de Saint Christophe et de Coivrel, *mais nous avons pris tant de soin à bien observer les autres angles, & l'Instrument donnait le tour d'horizon si justement, qu'il ne doit rester aucun doute là-dessus.* Picard donne le détail de ses résultats, sans indiquer les formules mathématiques utilisées ni ses méthodes de calcul.

Triangle ABC

Pour connaître le côté AC.
CAB 54° 4' 35"
ABC 95° 6' 55"
ACB 30° 48' 30"
AB 5663 toises de mesure actuelle.
Donc AC 11012 toises 5 pieds
Et BC 8954 toises

Triangle ADC

Pour connaître DC & AD
DAC 77° 25' 50"
ADC 55° 0' 10"
ACD 47° 34' 0"
AC 11012 toises 5 pieds
Donc DC 13121 toises 3 pieds
Et AD 9922 toises 2 pieds

Triangle DEC

Pour DE & CE

DEC 74° 9' 30"
DCE 40° 34' 0"
CDE 65° 16' 30" DC 13121 toises 3 pieds
Donc DE 8870 toises 3 pieds
Et CE 12389 toises 3 pieds

Triangle DCF

Pour DF
DCF 113° 47' 40"
DFC 33° 40' 0"
FDC 32° 32' 20"
DC 13121 toises 3 pieds
Donc DF 21658 toises

Triangle DFG

Pour DG & FG DFG 92° 5' 20"
DGF 57° 34' 0"
GDF 30° 20' 40"
DF 21658 toises
Donc DG 25643 toises 3 pieds
Et FG 12963 toises 3 pieds

De proche en proche, Picard détermine donc les longueurs des côtés de tous ses triangles.

La mesure d'un arc de méridien

Picard mesure un arc de méridien passant par Sourdon. Il connaît exactement la position des points V, N, I, G, E. Il doit déterminer la direction exacte du nord et utilise l'astronomie. Il se place à Sourdon en septembre 1969 et pointe, de nuit, sa lunette vers la polaire ; comme c'est une étoile proche du pôle (la précession des équinoxes change lentement cette position), elle décrit un petit cercle dans le ciel, donc un arc de cercle dans la nuit. Picard a placé une sorte de petit treillis de fils dans sa lunette (ces fils sont un peu éclairés pour pouvoir les distinguer dans la nuit) ; il suit la polaire jusqu'à sa *plus grande digression, où elle demeurait un espace de temps assez sensible sans sortir du filet vertical de la lunette* et bloque son instrument. Le matin, il peut déterminer la position du méridien par rapport aux autres éléments de sa figure. Il lui reste alors à projeter les points V, I, G, E sur le méridien (points $\beta, \gamma, \delta, \alpha$; l'arc α, β est un arc de méridien et Picard trouve sa longueur égale à 78 850 toises.

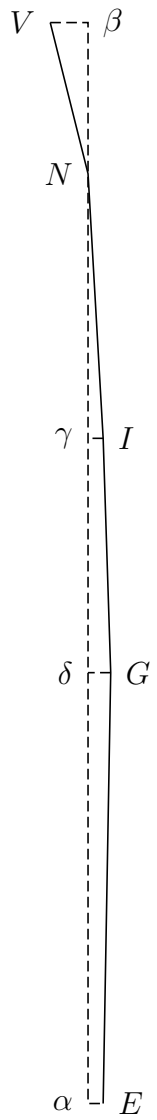


FIGURE 4.15 – Le calcul de la longueur de l'arc.

Picard détermine enfin avec beaucoup de soin les latitudes de V et E ; c'est une partie vraiment délicate car, comme le souligne Picard, une faible erreur sur les latitudes induit une forte erreur sur la longueur du méridien (1' d'erreur correspond à 951 toises). Picard obtient 1° 22' 55" pour l'arc de méridien entre Malvoisine et Amiens. Il peut ensuite terminer, comme nous l'avons déjà indiqué, le calcul de la longueur totale du méridien : $78850 \times \frac{1}{1 + 22/60 + 55/3600}$ qu'il arrondit pour diverses raisons à 57 060 toises.

4.8 Importance de la mesure de Picard

Le premier des Cassini : Jean-Dominique

En 1669, sur les conseils de l'abbé Picard, Louis XIV fait venir à l'Académie des sciences Jean Dominique (Gio Domenico) Cassini (1625-1712), le plus grand astronome de son temps ; Cassini dirige le nouvel observatoire que Colbert fait construire au sud du Paris de l'époque, devient français, épouse une française ; cinq générations de Cassini seront astronomes en France.

Cassini venait de publier, en 1668, des tables (*Ephemerides Bononienses mediceorum siderum*) indiquant l'heure exacte des éclipses des satellites de Jupiter (Cassini en donnera une seconde édition, plus précise, en 1693). Ces tables résolvent pour la première fois le problème de la détermination des longitudes en mer, si important pour les navigateurs. L'idée est la suivante : en observant l'éclipse d'un satellite au cours d'un voyage, un navigateur connaît grâce aux tables l'heure exacte qu'il est à Paris au même moment, puisque l'éclipse se voit au même moment aux deux endroits. D'autre part, l'observation du soleil lui permet de connaître le midi de l'endroit où il se trouve ; la comparaison des deux mesures de temps permet au navigateur d'en déduire sa longitude, donc sa position.

Ce moyen de connaître sa longitude est assez difficile en réalité à mettre en œuvre ; il fut abandonné un siècle plus tard, les horlogers réussissant à construire dans les années 1750 des horloges ne déviant pas de l'heure à laquelle elles ont été réglées pendant plusieurs mois.

Voir plus loin une conséquence extraordinaire des tables de Cassini.

Le voyage au Danemark

En 1671, Picard fait un voyage au Danemark. Il va dans lîle de Hven, là où Tycho Brahé avait son observatoire et constate avec tristesse qu'il n'en reste rien. Il fait la connaissance de Olaf Römer qu'il invite à Paris.

La mesure de la distance Terre-Soleil

En 1672, l'astronome Jean Richer fait le voyage de Cayenne. Le 5 septembre, il observe Mars, en même temps que Cassini à Paris. C'est le moment où le Soleil S, la Terre T et Mars M sont alignés dans cet ordre et où la distance TM est minimale, ce qui se produit tous les 15 ans environ ; O désigne de le centre de l'orbite de Mars.

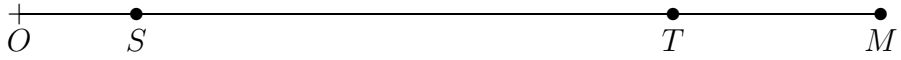


FIGURE 4.16 – La configuration lors des mesures de Richer et Cassini.

On sait en effet que l'orbite de Mars est elliptique et que le soleil en est un des foyers. La découverte de la forme elliptique Tycho-Brahé. Mais Tycho-Brahé avait conçu un modèle de système solaire où la Terre était fixe, où le Soleil tournait autour de la Terre et où les planètes autres que la Terre avaient des orbites circulaires. Il indiqua cette contradiction à Johann Kepler (1571-1630). Après plusieurs années de calculs, Kepler énonça ses fameuses lois (en 1609) décrivant les mouvements elliptiques des planètes autour du Soleil. Quatre vingts ans plus tard, Newton allait expliquer ces lois à partir de sa loi de gravitation universelle.

Le principe de la détermination de la distance TM au moment choisi par Richer et Cassini est très simple et s'appuie sur la mesure de Picard. On mesure au même moment à Cayenne C et à Paris P l'angle entre la direction de Mars et la direction d'une étoile très voisine E. On obtient des angles (très petits) MCE et PCE ; on en déduit CMP : c'est la somme de ces deux angles : il vaut 25".

La connaissance de la distance entre Cayenne et Paris, par la mesure de Picard, donne alors la distance de Mars à la Terre au moment des observations. Des calculs assez simples en utilisant les lois de Kepler permettent

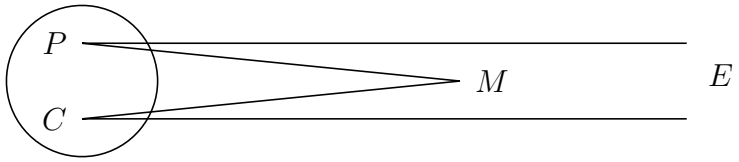


FIGURE 4.17 – Mesure de la parallaxe de Mars.

d'en déduire la distance de la Terre au Soleil ; le résultat de cette mesure (exprimé en toises à l'époque), publié en 1679, donne 146 millions de kilomètres, résultat très proche de la valeur actuelle, si c'est bien celui qui est obtenu (je n'ai pu le vérifier).

La vitesse de la lumière : Olaf Römer

Cassini avait bien observé des irrégularités dans ses tables, mais c'est Römer qui va, en 1975, jusqu'au bout des observations de Cassini. Considérons la figure suivante.

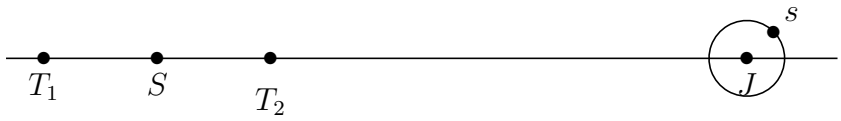


FIGURE 4.18 – Figure pour comprendre la démarche de Römer.

Dans la figure sont représentés le Soleil S, la planète Jupiter J, son satellite Io s et les positions T_1 et T_2 de la Terre diamétralement opposées et en alignement avec Jupiter. Römer constate que les tables donnent 16 minutes de différence entre les occultations de Io quand la Terre est en T_1 et quand la Terre est en T_2 ; il comprend que cette différence correspond au temps mis par la lumière pour parcourir la distance T_1T_2. Comme cette distance est maintenant connue, il devrait en déduire que la vitesse de la lumière est de 146 000 000 /16×60= 304 000 km par seconde (avec nos unités), mais la valeur citée par mes sources secondaires est 350 000.

La carte de France

Picard poursuit son travail sur la carte de France. La méthode des satellites de Jupiter lui permet de déterminer directement la position de nom-

breuses villes de France.

Le 6 février 1681, Picard envisage une carte de France précise obtenue avec ses méthodes de triangulation : *le dessein de faire la carte du Royaume par provinces, de la manière qu'on a commencé serait si long à exécuter qu'il n'y aurait pas lieu d'en voir la fin, il est certain que pour faire un bon assemblage de toutes les pièces après qu'elles seraient achevées, il en faudrait toujours venir à un châssis général, au lieu que ce châssis étant premièrement fait, il serait facile ensuite de le remplir... on pourrait commencer en faisant une route ou traverse depuis Dunkerque jusqu'à Perpignan qui sont à peu près dans le méridien de Paris...*. Picard meurt l'année suivante et ce n'est pas lui qui continuera cette énorme entreprise.

La prodigieuse conséquence pour la théorie de la gravitation universelle

Isaac Newton (1643-1727) avait commencé à réfléchir sur le mouvement des corps célestes vers 1666. Il comprend que les lois de Kepler peuvent se déduire d'une loi d'attraction proportionnelle aux masses et inversement proportionnelle au carré de la distance et que cette loi donne des trajectoires elliptiques dans le cas de deux corps. Mais quand il applique sa loi au mouvement de la Lune, il ne trouve pas les résultats escomptés. L'erreur vient d'un erreur sur la dimension de la Terre, Newton pensant qu'un arc de méridien d'un degré mesure 60 miles, soit entre 96 et 97 kilomètres. Il abandonne donc provisoirement sa théorie. Quand il prend connaissance de la mesure de Picard, en 1682, il refait les calculs et constatent qu'ils décrivent merveilleusement la réalité. Fortement aidé par Edmund Halley (1656-1742, l'homme de la comète), Newton rédige les *Principiæ*, une œuvre scientifique majeur qui paraît en 1687.

Ainsi la mesure de Picard, faite à partir de quatre bouts de bois sur une route d'Ille de France a-t-elle conduit à mesurer le système solaire, estimer la vitesse de la lumière et justifier une des grandes théories de la physique !

4.9 Après la mesures de Picard, quelques jalons

La suite de l'histoire est extrêmement longue, pleine de péripéties et d'avancées scientifiques ; mais j'ai choisi de faire un cours comportant des

sujets variés et je ne vais y consacrer que quelques pages.

La continuation de la carte de France

Le travail sur la carte de France est poursuivi par Jean-Dominique Cassini et Philippe de La Hire (1640-1718) est repris en 1683, interrompus par la mort de Colbert, reprises en 1700-01 avec l'aide de Jacques Cassini (1677-1756), le fils de Jean-Dominique, terminées en 1718 avec les fils Cassini et La Hire ; une chaîne de triangles est établie de Dunkerque jusqu'à Collioure, dans les Pyrénées orientales.

Les courtes périodes de travail indiquent une grande rapidité d'exécution ; en fait, surtout dans le midi, le travail n'est pas très soigné et est à l'origine d'une énorme polémique sur la forme de la Terre : les mesures des Cassini indiquent que la longueur du degré augmente quand on va vers le sud. Ainsi la Terre aurait la forme d'un ballon de rugby (si je peux me permettre la comparaison) tournant autour de son grand axe. C'est à l'opposé de ce que prévoient Huygens et Newton : si la Terre tourne sur elle-même, elle devrait être un peu aplatie aux pôles et enflée à l'équateur et plusieurs observations allaient dans ce sens.

Les travaux des ponts et chaussées dans les provinces du royaume demandent des cartes précises et le ministre Orry demande, en 1733, à Jacques Cassini et son fils César-François Cassini de Thury (17174-1784) de reprendre l'exécution de la carte de France. Ils commencent par mesurer des chaînes de triangles reliant Paris à Saint-Malo et, l'année suivante, Paris à Strasbourg. Le projet est cette fois poursuivi avec persévérance. Il aboutit à la fin du siècle : 182 planches, magnifiques ; la Bretagne est dans les dernières cartes.

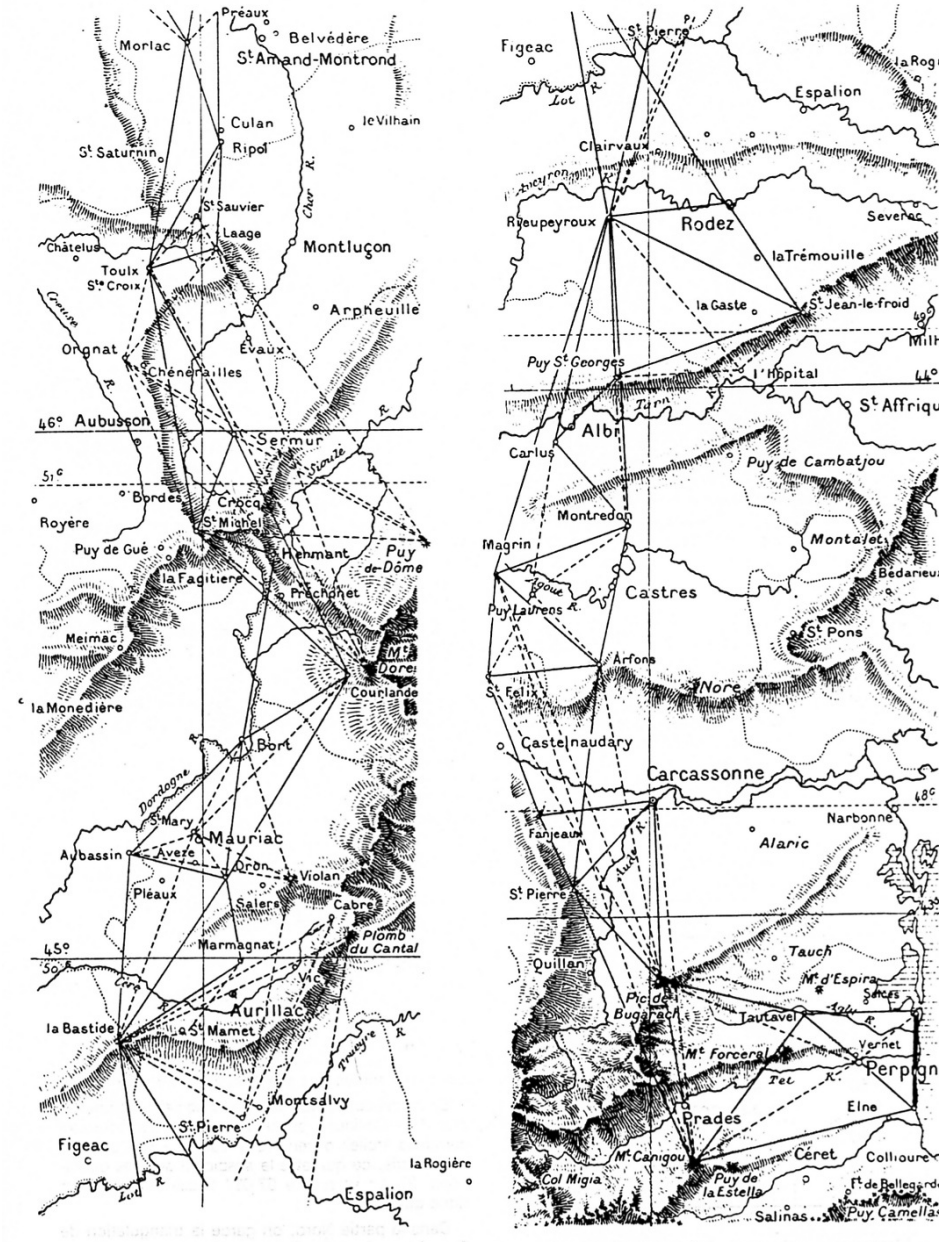


FIGURE 4.19 – La méridienne de Jacques Cassini.

FIGURE 4.20 – La méridienne de Jacques Cassini.

4.10 La forme de la Terre et les grandes expéditions

Presque tout le monde était convaincu de l'aplatissement de la Terre aux pôles ; la seule contradiction était les mesures des Cassini sur le méridien au nord et au sud de la France.

En 1735, on forme le projet d'aller mesurer un degré à l'équateur ; le ministre Maurepas soutient le projet pour la gloire de la France.

Une autre mission est décidée pour mesurer un degré de méridien au fond du golfe de Botnie, entre la Suède et La Finlande actuelle, le long de la rivière Tornea. Elle part en mai 1736, est assistée de l'armée suédoise ; Anders Celsius (1701-1744, celui qui inventa l'échelle de 0 à 100 pour les degrés de température, mais 0 correspondant à l'ébullition de l'eau et 100 à la glace fondante) vient l'assister. Une chaîne de triangles de 100 kilomètres est rapidement définies et les mesures d'angles sont faites en août. Les mesures astronomiques ont lieu début octobre. La base est mesurée sur le fleuve gelé (une idée de Celsius) en décembre, par un froid terrible. Des mesures complémentaires ont lieu au printemps 1737. L'expédition fait naufrage au retour sur la côte suédoise, mais tous les résultats peuvent être sauvés ; la toise étalon en sort rouillée. La mesure obtenue pour un degré de méridien à la latitude de 66° est 57 438 toises, plus grande qu'entre Paris et Amiens : la Terre est donc bien aplatie aux pôles.

La mission au Pérou devaient connaître des aventures autrement mouvementées ; en firent partie les académiciens Louis Godin (1704-1760), Pierre Bouguer (1698-1756) et Charles de La Condamine (1701-1774). Le voyage était déjà difficile : un bateau jusqu'à Panama, transport par terre jusqu'au Pacifique, autre bateau jusqu'en Équateur : plus d'un an de voyage (mai 1736-juin 1737). La mesure des chaînes de triangles fut acrobatique. Le terrain choisi comportait des dénivellations importantes (près de 2000 mètres). Godin travaille seul et refuse de communiquer ses résultats à ses deux collègues, voulant se réserver la primeur des résultats. Les difficultés s'accumulèrent : assassinat du chirurugien de l'expédition, querelles de femmes, dissensions avec le Vice-Roi, argent de France qui n'arrive pas et vente d'effets personnels, etc. Le retour est épique pour La Condamine, en 1743, qui franchit les Andes avec ses documents, redescend l'Amazone en canoë (plusieurs milliers de kilomètres), allant de mission en mission, franchissant les rapides, découvrant le caoutchouc... Le dernier à rentrer de l'expédition est le botaniste Jussieu, en 1771, après avoir herborisé pendant des années jusqu'au lac Titicaca.

Une retombée de cette expédition est la définition d'une unité de mesure précise pour les scientifiques : la toise du Pérou.

On trouve des livres magnifiques de l'époque (dans des bibliothèques municipales comme celle de Rennes) racontant toutes ces aventures.

Nous passons sous silence l'histoire des travaux des années suivantes pour arriver à la période révolutionnaire.

4.11 Le changement de système de poids et mesures à l'époque révolutionnaire

En 1790, les unités de surface, de capacité, de poids étaient en France d'une diversité incroyable.

Cela avait toujours existé et depuis toujours on avait envisagé d'y remédier : des réformes sont projetées durant tous les siècles précédents (depuis Charlemagne !), les dernières par Turgot et Condorcet en 1775.

On connaît dans la France entière les unités de longueur :

1 toise = 6 pieds ; 1 pied = 12 pouces ; 1 pouce = 12 lignes.

D'autres unités existent, spécifiques à des métiers, l'aune des drapiers par exemple.

Les unités de volume ne sont pas les mêmes suivant ce qu'on mesure. Pour mesurer les liquides, l'unité est le plus souvent la pinte, mais il en existe 11 valeurs en Ille-et-Vilaine, de 0,875 litre à Vitré à 1,359 litre à Saint Méen. Pour mesurer les céréales il existe 16 valeurs du boisseau à blé : il a une contenance de 2,515 litres sur les marchés de Rennes et c'est la plus petite valeur du département, 4,285 litres sur le marché de Saint Servan, 9,686 litres sur le marché de Combourg. Pour mesurer l'avoine et le blé noir en Bretagne, on utilise des boisseaux de contenances différentes : 3,041 litres à Rennes, etc. et ces boisseaux sont divisés suivant les régions en deux ou trois minots, etc.

Les calculs avec ces mesures n'étaient pas faciles et de nombreux traités d'arithmétique du XVIII$^{\text{Øme}}$ siècle y sont entièrement consacrés. Voici une addition du livre d'arithmétique du célèbre traité d'Étienne Bézout qui servira de base à la majorité des professeurs de mathématiques des écoles centrales années 1790 ; suivant les colonnes, les retenues ne se font pas de la même façon :

54	toises	2	pieds	3	pouces	9	lignes
12	toises	5	pieds	4	pouces	11	lignes
9	toises	4	pieds	11	pouces	11	lignes
8	toises	2	pieds	9	pouces	5	lignes
retenues	2		2		3		
85	toises	3	pieds	6	pouces	0	ligne

où les unités valent :

1 toise = 1,949 mètre
1 pied = 32,48 centimètres
1 pouce = 2,7 centimètres
1 ligne = 2,26 millimètres

Les soustractions, les multiplications et surtout les divisions posaient des problèmes beaucoup plus délicats : pour connaître le rapport entre deux mesures de l'addition précédente, il faut les convertir en lignes.

La réforme du système des poids et mesures a été entreprise par la Constituante en 1790 et c'est l'Académie des sciences, fondée par Colbert en 1666 comme on l'a vu, qui en a été chargée.

Celle-ci propose d'abord en octobre 1790 l'échelle décimale, déjà utilisée par les scientifiques : ce qui veut dire qu'on divisera désormais les unités en dixièmes, centièmes, millièmes et que leurs multiples seront dix, cent, mille fois plus grands. Les calculs sont ainsi mis à la portée de tous et les techniques de calcul sont celles qu'on enseigne aujourd'hui.

En mars 1791, au nom de l'Académie des sciences, Condorcet propose de choisir une unité de longueur prise dans la nature et basée sur la longueur du quart du méridien terrestre ce qui lui semble un argument décisif pour inciter les autres nations à l'adopter : la révolution cherche l'universel. Plus précisément, Condorcet propose de remesurer (cela donnera du travail aux académiciens) la distance de Dunkerque à Barcelone le long d'un méridien. Il faut un an pour construire les instruments très précis propres à effectuer la détermination de cette longueur et c'est pendant les journées insurrectionnelles de l'été 1792, vivant mille aventures, que Jean-Baptiste Delambre (1749-1822) et Pierre Méchain (1744-1804) commencent leurs mesures.

Le premier août 1793, la Convention, toujours décidée et expéditive, dans une séance où elle prend de multiples décrets organisant la défense de la France, balaie l'ancien sytème et en adopte un nouveau où tout est basé sur l'unité de longueur : le mètre. Elle ordonne la fabrication d'un étalon

provisoire basé sur des mesures antérieures du méridien, en attendant le résultat des mesures de Delambre et Méchain. Elle crée une commission qui rédige des instructions expliquant le nouveau système.

Le mètre provisoire aurait très bien pu devenir définitif, mais les mesures de Delambre et Méchain reprennent en avril 1795 pour être achevées 4 ans plus tard. Le mètre définitif diffère peu du mètre provisoire : 1/3 de millimètre. Des étalons des unités sont réalisés en 1799 et les savants de divers pays d'Europe sont associés avec solennité à leur consécration.

Il est faux de penser que le nouveau système ait été immédiatement adopté par les français. Comme pour les anciens francs, encore partiellement utilisés 50 ans après la création des nouveaux francs et les nouveaux francs qui s'enfoncent déjà dans le passé face aux nouveaux euros, l'usage des nouvelles mesures ne s'imposera en France qu'au milieu du XIX$^{\text{Øme}}$ siècle.

Bribes finales

Les travaux de géodésie ont pris une grande ampleur depuis 1800. Depuis 1957, les satellites artificiels donnent de nouveaux moyens de mesures ; les calculs sont très complexes car de nombreux paramètres apparaissent ; il s'agit de calculer pas à pas les mouvements décrits par des équations différentielles... Les applications sont multiples et il ne faut pas oublier que les militaires ont besoin de beaucoup de précision pour envoyer leurs fusées aux points qu'ils visent.

La victoire du mètre n'est pas complète aujourd'hui. Comme exemple particulièrement coûteux, on peut citer celui de la sonde américaine Mars Climate Orbiter perdue (des milliards de dollars) pour un problème de confusion d'unités : la société Lockheed avait fourni une partie de l'équipement où tout était programmé en unités anglosaxonnes, donnant des informations fausses dans l'approche de la planète rouge ; personne ne s'était aperçu de la difficulté dans les multiples essais au sol. Je crois aussi me souvenir qu'un robot martien a cru, là encore pour une confusion entre mètres et pouces, que le rocher vers lequel il se dirigeait était encore loin : il s'y est écrasé, et tu instantanément.

Rappelons aussi que Mars Polar Lander fut perdu le 3-12-1999 parce que les vibrations du déploiement des pieds de la capsule ont fait croire à l'ordinateur de bord que le sol martien était proche alors que la sonde était encore à 40 mètres d'altitude et que celui-ci a coupé les moteurs de freinage prématurément, entraînant la chute de la capsule qui s'est fracassée

sur le sol martien. Cette séquence n'avait jamais été testée car deux équipes s'occupaient de tester les procédures d'atterrissage, la première s'occupant du déploiement des pieds, la seconde de la suite et que la seconde, en réinitialisant les ordinateurs, ne pouvait s'apercevoir du problème !

La documentation sur cette dernière partie est très vaste, mais on ne peut tout faire.

Chapitre 5

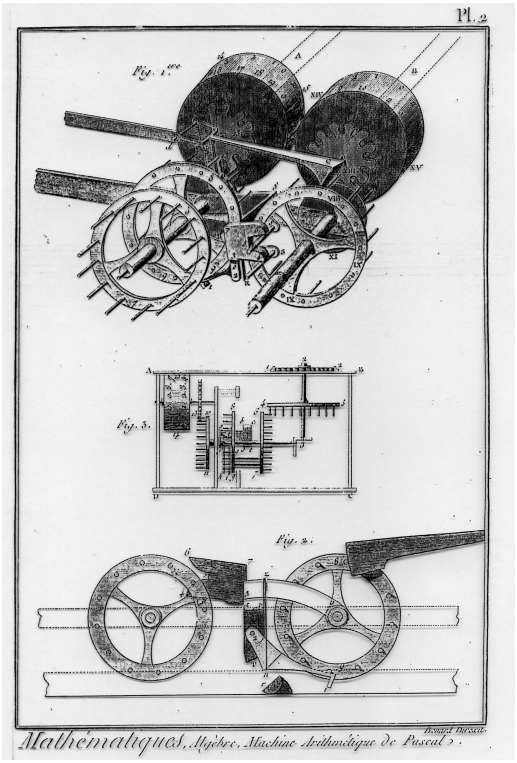
Histoire des calculateurs

5.1 La Pascaline

C'est certainement à Blaise Pascal (1623-1662) qu'on doit la première vraie machine à calculer, plus précisément à additionner et soustraire. La seule machine antérieure, une sorte d'horloge à poids construite en 1623 par Wilhelm Schickard, un astronome ami de Kepler, semble avoir été capable d'effectuer des additions, soustractions et quasi-automatiquement des multiplications, mais elle a brûlé en 1624.

Le père de Blaise, Étienne Pascal, est nommé commissaire délégué par le roi pour la levée des impôts et s'installe à Rouen le 2 janvier 1640 ; son fils l'aide pour les calculs longs et fastidieux liés à sa charge. Réfléchissant aux moyens d'alléger cette tâche, il étudie une machine permettant de faire facilement, rapidement et sans erreurs les calculs. Une cinquantaine de prototypes sont construits après beaucoup d'efforts et de réflexion. La difficulté principale était le problème des retenues dans les additions que Pascal résout au moyen d'un dispositif mécanique simple. Les premières machines ne comportaient que des roues décimales ; Blaise Pascal y adjoindra des roues vigésimales et duodécimales pour compter avec les unités monétaires de l'époque, la livre valant 20 sous et le sou 12 deniers.

La sœur de Pascal souligne le côté absolument nouveau de l'invention : *d'avoir réduit en machine une science qui réside tout entière dans l'esprit* et la possibilité de calculer sans *savoir aucune règle d'arithmétique*.



De nombreuses machines seront proposées par la suité pour améliorer le modèle de Pascal comme celle de Leibniz, en 1675, qui effectue des multiplications. Colbert lui en commandera trois attribuées significativement au Roi, à lui-même pour les finances du royaume, aux astronomes de l'Observatoire. Leibniz conçoit même en 1680 une machine où les nombres sont écrits en base 2 mais ne peut la réaliser. L'idée de codage en binaire est déjà présente chez Bacon en 1605 qui y voit les avantages de transmissions au moyen d'objets ne présentant que deux états.

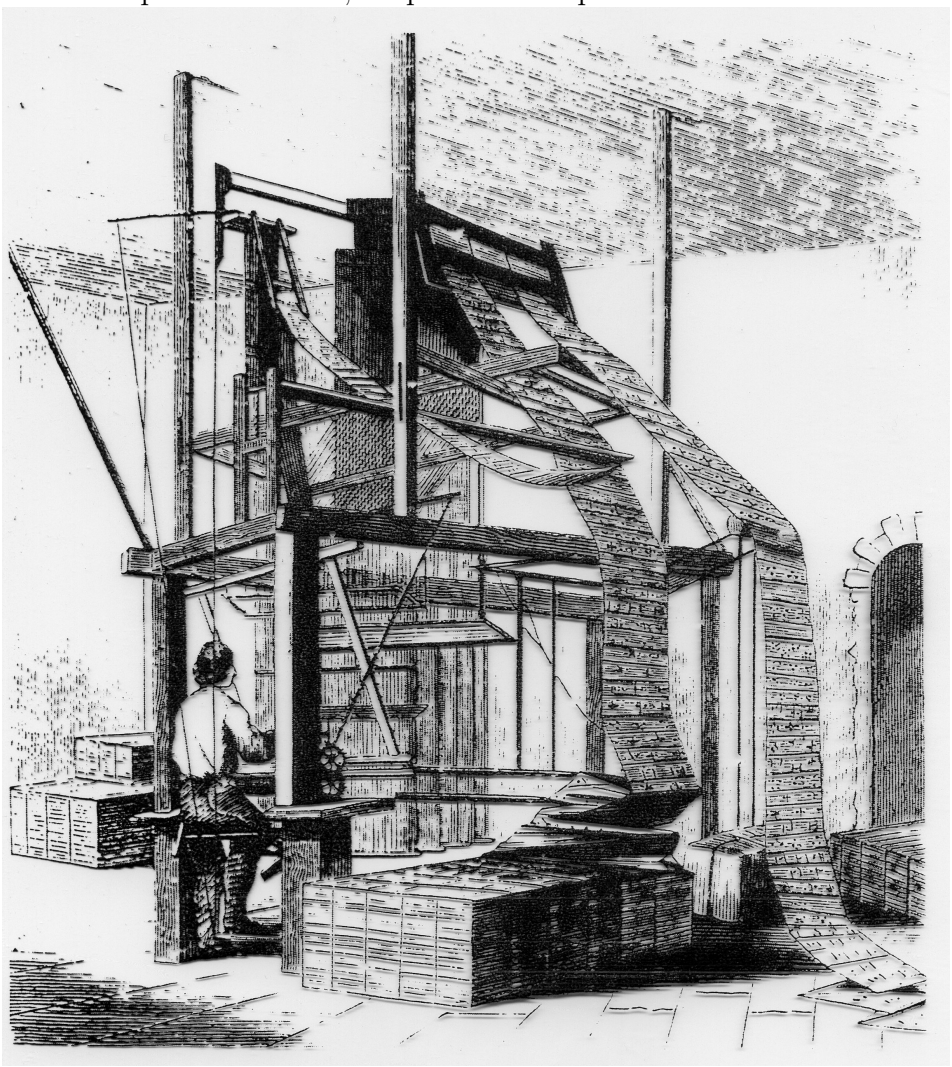
La règle à calcul est inventée en 1671 ; un siècle plus tard Cook l'utilise, estimant sa précision suffisante.

5.2 Le métier de Jacquard

Le 18ème siècle est le siècle de la construction de merveilleux automates et des progrès de l'horlogerie nécessaires pour la détermination précise des longitudes qui assure une navigation plus sûre. Dans un contexte tout à fait différent, l'automatisation des métiers à tisser conduit à l'invention de bandes

ou cartes perforées qui (B. Bouchon : 1725, J. de Falcon : 1728). Jacques de Vaucanson (1709-1782, le grand constructeur d'automates), de 1745 à 1755, perfectionne les métiers à tisser de Bouchon et Falcon, en les automatisant par hydraulique et en les commandant par des cylindres analogues à ceux de ses automates : 1745).

Jacquard construit , à la demande de Napoléon, le système en 1804 un métier à tisser révolutionnaire. Chaque carte commandait le filage d'une trame : seules les aiguilles en face des trous pouvaient passer pour actionner des crochets ; un empilage de cartes constituait un programme permettant de tisser une partie du tissu ; on pouvait le répéter si on voulait.



En 1812, 11000 métiers Jacquard fonctionnent en France. C'était la réalisation d'un rêve remontant à Aristote. La même année était conçu une version améliorée de la machine de Pascal : l'arithmomètre.

5.3 La machine de Babbage

Admirateur de Jacquard dont il conserve un portrait, l'anglais Charles Babbage (1792-1871) conçoit une machine : *la machine analytique* pleine d'idées fécondes mais qu'il ne réalisera jamais complètement. Dans ce projet, Babbage développe :

1) les unités d'entrée qui permettent d'indiquer à la machine l'algorithme à suivre ;

2) une unité de commande pour organiser l'exécution du travail dans la machine sans intervention extérieure, indiquant à la machine ce qu'elle doit faire en fonction des résultats qu'elle vient d'obtenir ou allant chercher un résultat dans la mémoire au moment opportun ;

3) une unité de mémoire, que Babbage appelle *store* et compare à un grenier à blé, pour stocker les résultats intermédiaires ou ceux à transmettre aux unités de sortie ;

4) une unité arithmétique et logique, que Babbage appelle *mill* (moulin) où il donne un rôle coissant aux cartes perforées de Jacquard, et qui peut itérer une séquence d'instructions ;

5) des unités de sortie pour afficher les résultats sous forme de cartes perforées, des dispositifs pour imprimer ou même pour tracer des courbes.

La fille de Lord Byron, Lady Ada Lovelace (1816-1852) est la première programmeuse du monde : elle écrit des programmes de calcul de fonctions mathématiques à partir des plans que lui adresse Babbage, critique les dispositifs qu'il imagine. Elle traduit, en 1842, en anglais le livre sur les travaux de Babbage rédigé par Ménébréa, un ingénieur militaire français qui avait rencontré Babbage à Turin, en 1840, où celui-ci exposait ses idées. Elle y ajoute de beaux commentaires : *la machine tisse les structures algébriques comme le métier de Jacquard tisse les feuilles*. C'est pour lui rendre hommage que Jean Ichbiah appelle ADA le langage de programmation développé pour le département américain de la défense en 1979.

La machine De Babbage est étudiée en 1878 par une commission dont Cayley : on propose de la modifier dans le but de calculer des déterminants, ce qui n'est pas une très bonne idée précise J.-L. Lions.

5.4 Nouveaux progrès

La machine conçue par Babbage est une machine numérique. A son époque, les machines analogiques représentaient l'avenir. Basées sur des propriétés mécaniques ou, à partir de 1912, sur celles du courant électrique, elles pouvaient calculer une fonction de manière continue ou déterminer ses coefficients de Fourier. Mais il y avait des difficultés :

1) contrairement à la machine numérique, il ne semble pas y avoir de montage universel qui permette de calculer une classe suffisamment large de fonctions ;

2) les résultats ne sont pas très précis ;

3) la mémorisation des résultats est difficile.

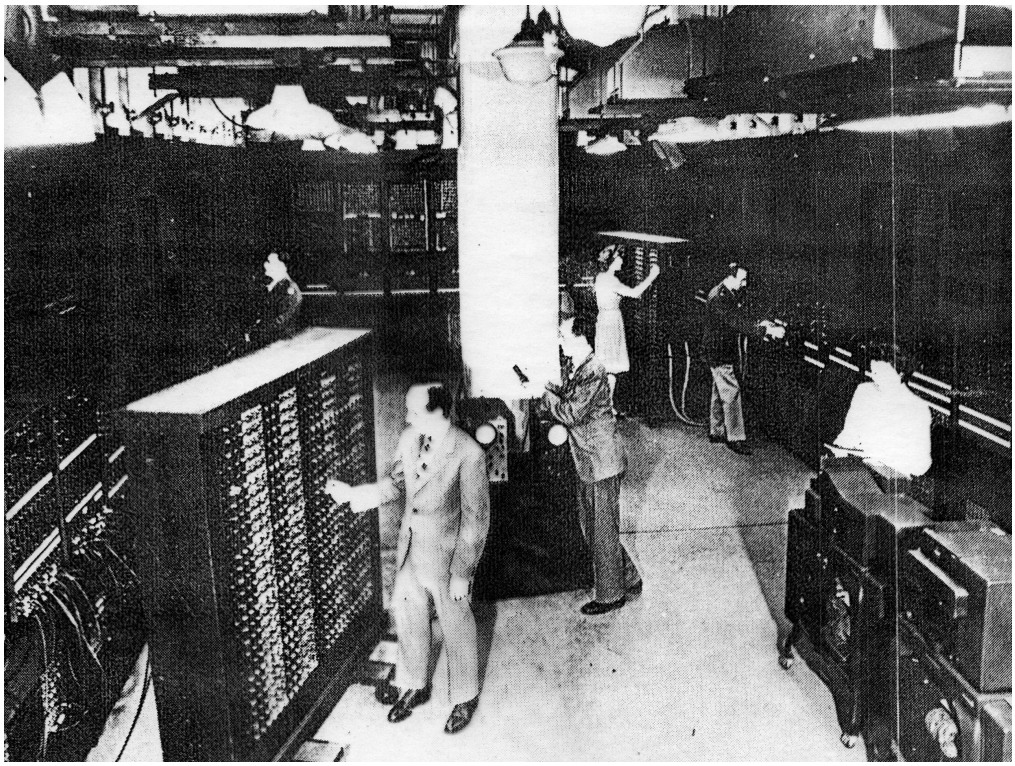
Une machine de ce type fonctionnera à Liverpool jusqu'en 1960 pour le calcul des marées.

C'est en 1889 que Léon Bollée, le fils du constructeur d'automobiles Amédée Bollée dont certaines voitures existent encore, construit une machine multipliant directement, sans additions successives, et c'est en 1912 que Monroë fabrique aux Etats-Unis une machine divisant directement.

Le début du 20ème siècle voit les progrès de la mécanographie, avec la mise au point de machines permettant de traiter les résultats de recensements, des problèmes de gestion ... Des sociétés qui fabriquent ces machines naissent la International Business Machine (IBM) en 1924, les machines Bull en 1933, du nom d'un ingénieur norvégien.

5.5 L'ENIAC et les premiers ordinateurs

Dans la conception des premiers ordinateurs, le rôle de mathématiciens de génie, tels John Von Neumann (1903-1957) et Alan Turing (1912-1954) est déterminant, en particulier pour la partie logique. Aux Etats-Unis, la construction de l'ENIAC (Electronic Numerical Integrator and Calculator) avait pour but le calcul numérique. Chaque décimale d'un nombre utilisait dix tubes.



La programmation consistait, au début (1946), à changer (et cela prenait parfois plusieurs jours) les positions des fiches sur le tableau de connexion ; la consommation d'électricité était énorme et éteignait, disent certains, les lumières de tout un quartier de Philadelphie, les insectes (bugs) qui se posaient sur les tubes (19000) provoquaient des pannes. La machine pesait 30 tonnes, son équivalent actuel pèserait moins d'un gramme, dépensait 150 kwh, on y faisait cuire des œufs sur le plat et elle occupait 160 m2.

L'effort de l'Angleterre pour décrypter les messages allemands codés par la machine ENIGMA avait conduit une équipe de plus en plus nombreuse (7000 personnes à la fin de la guerre) sous la direction, parmi d'autres, du mathématicien Alan Turing, spécialiste de la logique, à concevoir des machines adaptées à ce travail d'une importance extrême en temps de guerre. Les machines construites à Bletchley Park, Colossus à la fin de 1943, Colossus II le 31 mai 1944 sont parmi les premiers ordinateurs. Des problèmes mécaniques apparurent : fragilité des bandes de papier, inflammation dues à l'échauffement des relais qui conduisit à recourir à des tubes, etc. Cependant,

Colossus n'était pas prévu pour faire des multiplications...

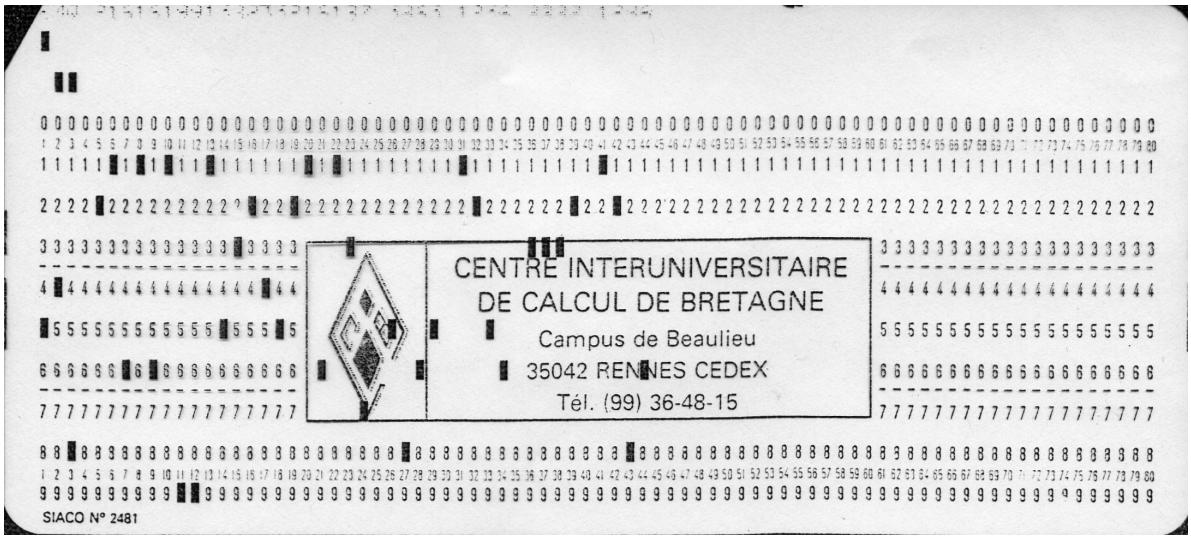
Des ingénieurs très dynamiques assurent au matériel français une place intéressante : F. H. Raymond constructeur du premier ordinateur français : CUBA pour l'Armée en 1952, M. Franklin, B. Leclerc, ..., P. Dreyfus (inventeur du mot : informatique), constructeurs des GAMMA chez Bull dans les années 50.

Les premiers langages sont proposés en 1958 : le FORTRAN dû à Backkus, le LISP dû à Mac Carthy. Le premier coprocesseur est fabriqué par Intel à partir de 1971.

5.6 La généralisation de l'informatique

C'est vers 1960 que l'industrie automobile commence à se doter de moyens informatiques. Par exemple, un jeune ingénieur de centrale se retrouve quelques mois aptrès son entrée chez Peugeot (il suffisait à l'époque de se présenter pour être embauché) à la tête du nouveau service des ordinateurs. La première machine était une IBM 650, machine décimale avec entrées et sorties uniquement par cartes qui effectuait une multiplication en 2 millisecondes, tambour stockant 150 000 bits d'information et tournant à 12 500 tours par minutes ; IBM l'avait commercialisée en 1953, pensant en construire 50 mais elle en vendit plus de 1000 et des améliorations furent apportées. Les premières applications portaient sur la gestion des chaînes et des salaires.

À Rennes, le premier calculateur est un IBM 1620 installé fin 1963 dans les locaux de la place Pasteur et surnommé Caroline. La première utilisatrice, Brigitte Cordier, met au point, sous la direction du professeur Jean-Paul Benzécri, les premiers programmes d'analyse factorielle des correspondance, méthode de représentations des données qui a connu depuis des développements considérables et est à l'origine de ce qu'on a appelé l'Ecole française d'Analyse des données. Les cartes perforées se coinçaient et, pour les récupérer, les épingles à cheveux trouvaient un usage inattendu.



La présence d'un curé était incompatible avec le fonctionnement de l'ordinateur : sa soutane bouchait immanquablement la climatisation, la température montait et Caroline refusait sur le champ de continuer à travailler.

Les machines de l'époque étaient compliquées, souvent en panne : il fallait aller de nombreuses semaines chaque année en stage chez le constructeur (IBM le plus souvent), faire venir des techniciens très compétents pour les pannes diverses qui survenaient incessamment.

Pour finir ce chapitre, notons que les premiers langages sont conçus en 1958 : Backkus conçoit le Fortran et Mc Carthy le Lisp). Le premier coprocesseur est fabriqué par Intel en 1971. Quant au développement d'Internet, aux communications entre ordinateurs, c'est une vaste histoire commencée vers 1960.

Chapitre 6

Vannevar Bush, les mathématiques et la guerre, autour de 1940

6.1 Vannevar Bush (1890-1974)

Vannevar Bush est surtout connu aujourd'hui pour ses idées novatrices sur l'organisation de l'information publiées dans son célèbre article de juillet 1945 : *As we may think*, mais le reste de ses travaux et de ses activités mérite d'être connu.

Vannevar Bush

La thèse de Bush, en 1913, porte sur la géodésie : il invente le *Profile Tracer*, un appareil consistant en une boîte montée sur deux roues de bicyclette qui permet de tracer sur un cylindre le profil d'un terrain accidenté.

Pendant la première guerre mondiale, Bush travaille pour la Navy pour les problèmes de détection de sous-marins.

Bush s'intéresse à la résolution graphiques des équations différentielles. À cette époque, *Pour l'intégration des équations différentielles ordinaires, ce sont les méthodes graphiques qui sont les plus rapides et les plus claires* (Runge et Willers, 1915, *Numerische und graphische Quadratur und Integration gewöhnlichet und partieller Differentialgleichungen*, *Encyklopädie der mathematischen Wissenschaften mit Einschluss ihrer Anwendungen.*) La prépondérance de ces méthodes s'explique facilement alors que les ordinateurs n'existaient pas et que des calculs approchées avec des tables de logarithmes eussent été trop coûteux en temps. Il faut penser qu'un problème de physique conduit rarement à une équation différentielle facilement intégrable comme celles qu'on enseigne aux étudiants de première année d'université.

Bush publie deux articles sur le sujet en 1927 et présente, en 1931, son *Differential analyzer*, une machine complexe pour résoudre graphiquement des équations différentielles dont les capacités dépassent celles des intégraphes existants.

Bush travaille aussi sur des appareils d'optique et de photocomposition

et sur un appareil de sélection rapide pour des banques de microfilms.

En 1932, Bush est nommé vice-Président du MIT ; en 1938, il est président de l'Institut Carnegie à Washington ; en 1939, il est nommé à la tête du National Advisory Committee for Aeronautics (il le restera jusqu'en 1948) ; en juin 1940, le NDRC, National Defense Research Commitee, pour le dévelopement de nouvelles armes, est créé par Roosevelt sur les conseils de Bush. Bush est appelé à le diriger tout en conservant la présidence de la fondation Carnegie. En 1941, l'OSRD, Office of Scientific Research and Development, pour coordonner les travaux des scientifiques et des techniciens dans l'effort de guerre, est créé. Cet organisme inclue le NDRC et Bush en prend la direction jusqu'en 1946. Il sera responsable de l'organisation du travail de 6000 scientifiques impliqués dans l'effort de guerre. Bush est donc un personnage central du développement des recherches sur la fission nucléaire et du projet Manhattan. C'est lui qui persuade le président de débloquer 2 milliards de dollars pour la construction de la bombe atomique. Il s'occupe aussi des travaux sur les antennes de radar, sur les tables d'artillerie et du dévelopement des premiers ordinateurs.

En 1944, Roosevelt demande à Bush des recommandations pour les activités en temps de paix tirant les leçons de la guerre, pour la santé, la création de nouvelles entreprises créant des emplois, l'amélioration du niveau de vie. C'est l'origine du célèbre article de juillet 1945 : *As we may think* (il y propose le Memex) et du rapport : *Science the endless frontier*. Bush y souligne l'importance de la recherche fondamentale comme base capitale de toute recherche appliquée. Ce rapport conduira à la création de la National Science Foundation en 1950.

Bush fait partie d'une commission intérimaire chargée d'établir s'il convient ou non de recourir à l'arme atomique (commission comprenant quelques membres de l'Administration : Stimson, le général Marshall, James F. Byrnes, futur secrétaire d'État de Truman, trois savants : Vannevar Bush, James Conant, Karl Compton, les principaux physiciens du Projet Manhattan : Oppenheimer, Fermi, E. O. Lawrence, Arthur H. Compton. Les discussions sont difficiles devant la résistance du Japon, le coût énorme de l'invasion du Japon en vies américaines, etc. Le 16 juillet 1945, Bush assiste à l'explosion de la première bombe atomique sur le site de Trinity à Alamogardo, au Nouveau Mexique. On raconte qu'il aurait été victime d'un malaise nerveux ; une photo le montre l'air fermé ou songeur, serrant la main de James Conant.

L'article *As we may think* est publié en juillet 1945 dans la revue *The Atlantic Monthly*. Une version abrégée paraît dans Life.

Quand il écrit cet article, Bush utilise la connaissance approfondie des recherches qui ont été poursuivies, de leurs résultats, de leurs applications militaires, mais il ne peut en parler directement, les secrets doivent être gardés. En particulier, il ne peut parler des premiers ordinateurs, comme l'ENIAC, dont l'existence ne sera révélée que le 16 février 1946, par le New York Times, mais il anticipe les développements que permettront leurs successeurs. La première bombe atomique n'a pas encore explosé. Il décrit l'avenir à partir des possibilités de son époque, un peu comme dans les romans de Jules Verne. Les scientifiques ont participé à l'effort de guerre, abandonnant leur ancien modèle de fonctionnement en compétition les uns avec les autres. Que vont-ils faire maintenant ? Si les médecins et les biologistes pourront revenir à leurs objectifs antérieurs, il n'en est pas de même pour les physiciens et les chimistes qui ont conçu des armes destructrices (rappelons que Bush écrit avant la première explosion atomique) qui ont repoussé les ennemis, mais dont les nouveaux objectifs sont à définir.

Bush analyse les nouvelles conditions de travail du chercheur : il va devoir faire face à une masse de connaissances qu'il ne pourra toutes consulter faute d'accès, faute de liens entre les différentes connaissances. Il cite l'exemple des lois de Mendel, publiées en 1866, mais ignorées jusqu'en 1900 et veut faire en sorte que de telles catastrophes ne se renouvellent pas. Bush évoque tous les nouveaux moyens de rendre accessibles des informations : photographies, microfilms, la nouvelle télévision, etc. Il imagine l'environnement dans lequel pourrait travailler le scientifique : environné d'appareils lui apportant les informations, lui permettant de les trier à grande vitesse, entourés de pièces pleines de femmes en train de perforer des cartes pour effectuer les opérations répétitives (*One of them will take instructions and data from a roomful of girls armed with simple keyboard punches*), les calculs arithmétiques et statistiques, opérations auxquelles Bush ajoute les opérations logiques. Bush imagine des machines sélectionnant parmi des millions de données celles qui nous intéressent, des machines gérant entièrement de grands magasins : entrée et sorties de produits, clients, etc.

Le cœur du problème est le classement des données. L'ordre alphabétique ou numérique ne suffit pas, d'autres types de recherche sont possibles et le cerveau humain ne procède pas ainsi ; le cerveau fonctionne par associations successives rapides et il faudrait concevoir une machine qui en imite le fonctionnement. Bush nomme Memex la machine qu'il imagine pour cela. On pourrait y stocker tous les livres (je note que c'est un projet bien avancé aujourd'hui) ; la machine serait consultable rapidement, souplement, simple-

ment et éventuellement à distance. Elle disposerait d'écrans de visualisation, de clavier, de boutons, de leviers. L'archivage serait automatique, l'accès à une information serait possible à partir de mots clés, elle pourrait redonner les informations précédemment consultées, elle pourrait trouver des informations associées. Une caméra adjointe à la machine serait capable de photographier tout ce qui serait jugé intéressant, le rendant immédiatement disponible sur la machine. Une autre machine pourrait écrire ce qu'on dirait.

On peut remarquer que l'ambition de Bush de stocker des masses énormes d'information allaient bien au-delà du seul ordinateur de l'époque, l'ENIAC, et anticipe nos mémoires actuelles qui atteignent des dizaines de gigaoctets (si je ne me trompe) sur l'ordinateur le plus banal.

Le projet de Bush était bien fait pour stimuler la recherche dans la paix retrouvée. Un colloque a été organisé pour célébrer le cinquantenaire de l'article de Bush à l'Université de Brown, les 12 et 13 octobre 1995. Les orateurs prévus étaient : Douglas Engelbart, Theodor Nelson, Robert Kahn, Tim Berners-Lee, Michael Lesk, Nicholas Negroponte, Raj Reddy, Lee Sproull, Alan Kay, tous reconnaissant l'importance de l'article de Bush. Douglas C. Engelbart (né en 1925) est l'inventeur, en 1970, de la souris, pour laquelle il n'a jamais rien touché. En 1963, il crée AUGMENT à Stanford, le plus ancien système hypertexte. Dans ce système, la souris, les ouvertures de fenêtres multiples, les pointeurs, les graphiques intégrés sont plein de potentialités que le livre, à la structure linéaire, ne permet pas. Personne ne pensait alors à l'ergonomie ni aux représentations graphiques, l'ordinateur était vu comme une armoire. Theodor Holm Nelson (né en 1937) crée le mot hypertext en 1965. Son système Xanadou, du nom du palais où l'empereur Kubilai Khan entassait ses trésors et qu'on retrouve dans Citizen Kane avec la même fonction, est une sorte de banque d'informations illimitée où tout ce qu'on cherche et tout ce qui est associé à ce qu'on cherche est est accessible. Il accepte l'incorporation de nouvelles données par les utilisateurs. Chacun reçoit de l'argent quand les données qu'il a déposé sont utilisé par d'autres, etc. On est sur la voie de la technologie du World Wide Web, 25 ans avant sa création. Timothy (Tim) Berners-Lee est né à Londres. Chercheur au CERN, il crée le premier site internet, d'abord interne au CERN, en décembre 1990, puis sur la toile, le 6 août 1991 : http ://info.cern.ch/. Il travaille actuellement au MIT.

6.2 La balistique extérieure

La balistique extérieure étudie le mouvement du projectile à partir de sa sortie du canon (la balistique intérieure étudie le mouvement du projectile à l'intérieur du canon, elle est extrêmement délicate).

La résistance de l'air est ce qui pose problème, elle n'est connue que de façon empirique, et elle dépend de multiples facteurs, comme ceux indiqués par Goldstine et que nous citons ci-dessous. Le cas particulier du vide où $F(v) = 0$ s'intègre sans difficulté et a été résolu par Galilée. Dans les autres cas, les méthodes d'intégration graphique étaient bien adaptées. Newton, Euler, Jacobi ont envisagé différentes modélisations de la résistance de l'air, mais éloignées de la réalité physique pour les besoins du calcul.

Les tables d'artillerie

Goldstine écrit que le calcul des tables d'artillerie et de bombardement a été la *raison d'être* (en français dans son texte) du premier calculateur électronique. Il décrit la situation d'un artilleur à son poste : il connaît la position de la cible qu'il a à atteindre par sa direction et sa distance. La table d'artillerie lui indique quelle doit être l'inclinaison de son canon et quelle doit être la correction par rapport à la direction de la cible, autrement dit la correction par rapport à l'azimuth de la cible. De nombreux paramètres sont en jeu : la direction du vent, sa vitesse, la densité de l'air, la température, l'altitude, le poids de l'obus, le poids de la charge... Les tables étaient imprimées sur de petits livrets tenant dans la poche. De nouveaux usages du canon apparaissent durant la deuxième guerre mondiale car la cible peut être un avion : le réglage du tir doit alors être très rapide et des appareils automatiques de réglage furent mis au point, qui tenaient compte de la localisation par un radar et des divers paramètres du tir.

6.3 Mathématiques et bombe H

Un des aspects de la conception de la bombe H est exposé dans l'article :

Galison Peter, Les nombres, la bombe H et la simulation du réel, in *Les sciences pour la guerre*, Ecoles des hautes études en sciences sociales, 2004.

L'histoire se joue entre quelques très grands scientifiques de l'époque : Von Neumann, Stanislaw Ulam, Enrico Fermi,

En 1946, une réunion de physiciens discutent d'un projet d'arme utilisant l'énergie de fusion des atomes d'hydrogène. L'effet devrait être comparable à celui d'événements naturels comme l'éruption du Krakatoa ou le tremblement de terre de San Francisco.

Toute la physique théorique pouvait servir à la conception de la nouvelle bombe. Mais les réactions deutérium-deutérium, deutérium-tritium, la dissipation de l'énergie résultant des réactions, l'hydrodynamique de l'explosion, etc. étaient inconnues dans des conditions extrêmes proches de celles du noyau solaire.

Les méthodes analytiques étaient en échec devant la complexité des équations ; aucun phénomène comparable à une échelle plus petite n'existait.

L'outil pour faire des calculs numériques venait d'être construit ; c'était l'ENIAC, le seul ordinateur existant. Il avait été conçu parce que les calculs du projet Manhattan avaient rendu nécessaires de telles machines. Mais dans le cas des calculs pour la nouvelle bombe, il se révélait encore insuffisant. Les équations différentielles décrivant le fonctionnement de la future bombe, calculées par Metropolis et ses collaborateurs, étaient très complexes et l'ENIAC, en produisant une carte perforée par seconde, n'avançait pas dans les calculs.

Il fallait donc d'abord trouver des méthodes nouvelles pour rendre les équations abordables par le calculateur. Ulam commença à élaborer la méthode de Monte-Carlo ; un court article en commun avec Von Neumann, de 1947, présenta pour la première fois l'idée de la méthode. Il s'agissait de simuler au hasard des événements et de regarder ce que donnaient les équations. Ulam et Everett parvinrent à programmer l'ENIAC pour conduire des calculs sur un modèle simplifié de la bombe H en 1949 et le programme fut installé sur l'ENIAC début 1950. Les premiers résultats furent décevants, indiquant que la détonation ne pouvait pas se produire. Ulam écrivit à Von Neumann que l'hydrodynamique était le seul espoir que ça finisse par marcher.

Parallèlement, Ulam et Von Neumann obtiennent le feu vert de Truman pour la construction de la bombe et des crédits sont débloqués.

Pendant ce temps, un fort courant militait pour que la bombe H ne soit pas construite : Einstein passait à la télévision, Hans Bethe affirmait que le niveau de destruction envisagé était comparable à un génocide et espérait qu'elle ne pourrait jamais être construite. Le chimiste Harold Urey souligna que, si les Russes parvenaient les premiers à construire la bombe H, cela leur donnerait la possibilité de poser des ultimatums insupportables ; seule une puissance démocratique, avec des libertés, etc. méritait de posséder cette

arme. Bethe répondit que la question la plus importante était une question morale : pouvait-on introduire une arme d'annihilation totale ? Teller était évidemment favorable à la bombe. Ulam trouvait ces discussions assez drôles et poursuivait ses calculs, qui montraient que la bombe n'exploserait pas, se disputait avec Teller, qui avait une idée différente.

Entre le 18 et le 25 janvier 1951, Ulam eut l'idée de génie : il imagina une nouvelle configuration de la bombe, on ne chercherait plus à créer les énormes températures exigées avec une bombe à fission, on utiliserait la bombe A pour créer des pressions énormes sur le matériau fusible, ce qui éviterait des dégagements de chaleur extrêmes.

Il ne restait plus à Ulam qu'à convaincre Teller et ses collègues. Le GAC revint sur son opposition de 1951 à la bombe, Bethe cessa de s'opposer. Tout le monde se mit au travail, Teller, Bethe, etc. pour terminer le travail de conception. La première bombe H explosa le 30 octobre 1952 dans le Pacifique sud, dans l'île d'Eniwetok, qui fut rasée.

Von Neumann continua d'utiliser la simulation Monte-Carlo dans de multiples problèmes comme ceux de la prévision météorologique.

Un détail peut être donné. Pour obtenir des suites de nombres au hasard, Ulam et Von Neumann eurent l'idée de partir d'un nombre de 10 chiffres, de l'élever au carré, de conserver les 10 chiffres du milieu et de recommencer. Bien sûr, cela ne donnait pas une suite infinie de nombres au hasard, puisqu'il n'y avait qu'un nombre fini de nombres de 10 chiffres et que le processus bouclait. Mais Von Neumann expliquait qu'il avait besoin d'un millier de nombres au hasard et que, cela, sa méthode lui donnait parfaitement.

On remarquera aussi le caractère expérimental de la méthode : la stabilité des résultats n'est assurée que par la similitude des résultats après plusieurs calculs. Le Monte-Carlo fut l'objet de nombreuses applications dans des domaines variés et de nombreuses discussions sur la validité de son application en physique, etc.

Citations

Je voudrais donner quelques citations et commentaires plus personnels. D'abord, quelques citations qui se font écho :

Plaisante justice qu'une rivière borne. Vérité au-deçà des Pyrénées, erreur au-delà. (Pascal)

Il devient honorable de tuer un homme s'il habite de l'autre côté de la rivière... C'est ainsi, ces absurdités font l'histoire. (Pascal)

Seigneur, faites de moi un instrument de paix. Là où est la haine, que je mette l'amour, là où est l'offense, que je mette le pardon, là où est la discorde, que je mette l'union. (Saint François d'Assise)

Je suis particulièrement choqué par des épisodes comme le suivant, qui montrent que les scientifiques ont des attitudes diverses. En 1965, passant outre les diverses conventions internationales sur la guerre, les États-Unis utilisèrent au Vietnam des armes qui tuaient ou blessaient les populations civiles sans discrimination. Les bombardements au phosphore ou au napalm étaient suivis de bombardements avec des bombes à fragmentation ou des bombes à billes. Un comité de scientifiques américains dont plusieurs prix Nobel, le Comité Jason, mit au point de nouveaux armements, en particulier les bombes à fragmentations en plastique, dont les éclats étaient indécelables aux rayons X, rendant plus difficiles leur extraction. Devant la barbarie des moyens mis en œuvre, le mathématicien et philosophe anglais Bertrand Russel fonda un tribunal pour enquêter sur ces crimes de guerre et les dénoncer devant l'opinion publique internationale. Laurent Schwartz, ami de Russel, participa au Tribunal Russel et popularisa son action en France.

Chapitre 7

Médailles Fields

Les médailles Fields (du nom d'un mathématicien canadien) sont considérés comme l'équivalent en mathématiques des prix Nobel [1].

7.1 Pourquoi n'existe-t-il pas de prix Nobel en mathématiques ?

Alfred Nobel (1833-1896), fils d'un ingénieur chimiste, est un chercheur très brillant, auteur de nombreuses inventions. Il est devenu richissime par le développement, en Europe et aux Etats-Unis, de ses usines chimiques et d'armement ; c'est lui qui invente la dynamite en 1866 permettant d'utiliser les propriétés d'explosif de la nitroglycérine (inventée en 1847 par l'italien Sobrero) : par adjonction d'une terre siliceuse, le kieselguhr, il forme une pâte. Les bâtons de dynamite révolutionne les exploitations minières, la construction de routes, de voies ferrées, le percement de tunnels (Saint-Gothard) et de canaux (Panama, Corinthe), etc. Les expérimentations de Nobel sont dangereuses : une explosion cause la mort de son jeune frère Emil et de bien d'autres personnes.

Outre les disciplines scientifiques, la littérature et la lutte pour la paix dans le monde ont été au centre des préoccupations de Nobel (il pensait que l'invention d'un explosif très puissant dissuaderait à jamais les humains de se faire la guerre). Par testament du 27 novembre 1895, il propose la création d'une fondation, financée par une partie de sa fortune, pour récompenser

1. Parmi mes sources, l'article de Francis Casiro, Tangente n° 76, août-septembre 2000

chaque année des chercheurs (quelle que soit leur nationalité) en physique et en chimie, en médecine, des écrivains (auteurs d'œuvres de tendance idéaliste) et des militants pour l'abrogation des armées permanentes et la promotion de congrès pour la paix. Les cérémonies ont lieu à Stockholm le 10 décembre, date anniversaire de sa mort, en présence du roi de Suède, à l'exception de la remise du prix Nobel de la paix qui a lieu à Oslo.

Mais pourquoi Nobel n'a-t-il pas créé de prix en mathématiques ? Il semble que ce soit tout simplement parce qu'il ne s'intéressait pas à elles. On peut lire à ce sujet l'article de Lars Gårding et Lars Hörmander dans *The mathematical intelligencer*, 1985, volume 7, n° 3, page 73, qui enterrent une version, française ou américaine, selon laquelle la véritable raison serait le dépit de Nobel après un échec dans une rivalité amoureuse (notons que Nobel n'a jamais été marié, contrairement à ce qu'on trouve parfois écrit) avec le mathématicien suédois Mittag-Leffler, version dont l'avantage était de fournir un sujet de discussion inépuisable aux mathématiciens du monde entier en leur permettant d'expliquer cette inégalité frustrante avec la physique, la chimie, etc. Cependant, on sait que les relations entre Mittag-Leffler et Nobel ne s'appréciaient pas...

En fait, il y eut peu de femmes dans la vie de Nobel. Il vit pendant huit jours en 1875, une liaison passionnée avec la comtesse Bertha von Kinsky, venue de Vienne pour être sa secrétaire. Celle-ci est une grande militante de la paix ; elle entretiendra une longue correspondance avec Nobel qui est probablement à l'origine de la création du prix Nobel de la paix. Elle ne croyait pas à l'idée d'équilibre de la terreur de Nobel et proposait de tenir des congrès de la paix et d'éduquer les peuples. Elle reçut le prix Nobel pour son action inlassable en faveur des idées pacifistes en 1905.

Un prix Nobel d'économie existe depuis 1968. Parmi les lauréats, en 1994, le grand mathématicien américain John Nash, connu du grand public par le livre et film récents *Un cerveau d'exception* (mais ayant connu de grosses difficultés psychologiques) pour des résultats de théorie des jeux de plus en plus utilisés aujourd'hui.

7.2 Médailles Fields

En 1924, le congrès international des mathématiciens avait lieu à Toronto ; les mathématiciens de l'Allemagne et de ses alliés durant la guerre de 1914-1918 n'y étaient pas invités. Le Président était le mathématicien

canadien John Fields (1863-1932) et la collecte de subventions avait été particulièrement fructueuse. Fields proposa que l'argent restant serve à financer des médailles (deux tous les 4 ans) pour les mathématiciens de toutes les nationalités, sans exclusive. On ne sait si les liens personnels de Fields avec Mittag-Leffler ont joué un rôle dans cette proposition.

Ce n'est qu'en 1932, au congrès de Zürich que la communauté mathématique mit l'idée de Fields, qui venait de mourir mais avait laissé une longue lettre, en place. Fields avait laissé pour financer les médailles une partie de sa fortune, en plus des fonds récoltés en 1924.

Les Médailles Fields (Fields n'avait pas proposé de nom pour ces médailles en or) sont décernées tous les quatre ans lors du congrès international des mathématiciens à des chercheurs (au moins deux, quatre au maximum, de moins de quarante ans par tradition, la conséquence étant que les médaillés d'après 1950 sont presque tous vivants, ce qui n'est pas le cas des prix Nobel) qui ont obtenu des résultats jugés importants, nouveaux, très difficiles, ouvrant sur des développements futurs, par la communauté mathématique. Elles ont été décernées pour la première fois en 1936, et régulièrement (à l'exception de 1982) depuis 1950. Un prix modique de 1500 dollars les accompagne.

Dans le palmarès, on remarquera 8 chercheurs de l'école mathématique française et deux belges qui en sont proches, signe de la grande qualité de la recherche mathématique dans nos contrées ! Seuls les Etats-Unis font mieux ! L'Ile de France abrite la plus forte communauté de mathématiciens du monde, mais cette prépondérance est menacée par les budgets français actuels qui ne permettent pas le remplacement total de ceux qui partent à la retraite.

Dans la liste qui suit, on essaie de dire un mot des travaux des médaillés, ce qui n'est pas facile, mais intéressera peut-être quelques personnes. On peut compléter l'information sur chacun de ces médaillés par une recherche sur le réseau ; certains des plus récents d'entre eux ont même des sites qu'on peut consulter et où sont rassemblés leurs travaux.

1936

Lars Ahlfors (Finlande, 1906-1997)

pour ses contributions à la théorie des fonctions de variable complexe et des surfaces de Riemann.

Jesse Douglas (Etats-Unis, 1897-1965)

pour la résolution du problème posé par le physicien belge Plateau (déjà posé par Lagrange en 1760) : problème de l'existence de surfaces d'aire minimale dont le bord est une courbe fermée donnée ; problème qu'on peut présenter simplement avec le dispositif suivant : la courbe fermée est matérialisée par un fil de fer et un film de savon qui s'appuie dessus, comme dans les jeux de notre enfance, donne une surface d'aire minimale.

1950

Laurent Schwartz (France, 1915-2002)

(Cette section, comme d'autres, est reprise de mon petit livre de la collection TOPOS, chez Dunod.)

Laurent Schwartz (1915-2002)

Dans un très beau livre (*Un mathématicien aux prises avec le siècle*, Odile Jacob, 1997), Laurent Schwartz retrace son itinéraire de mathématicien, d'homme et sa vie de militant contre les injustices. La période de la guerre est extrêmement difficile pour Schwartz, d'origine juive. Schwartz invente les distributions (une généralisation de la notion de fonction, comme la *fonction* δ de Dirac, nulle partout sauf en 0 où elle est infinie et telle que $\int_{-1}^{1} f(t)\delta(t)\,dt = f(0)$), maintenant d'un usage constant dans les mathématiques appliquées et certaines branches de la physique. Il reçoit la médaille Fields en 1950.

Schwartz organise, avec d'autres, la soutenance de thèse *in abstentia* de Maurice Audin, jeune mathématicien arrêté, torturé et assassiné par l'armée française à Alger en juin 1957. Il signe le manifeste des 121 ; c'est lui aussi qui est à la tête des comités Vietnam en 1965, qui propose à Grothendieck d'aller y donner des cours sous les bombes en 1969.

Schwartz avait une singularité : il était incapable de voir dans l'espace, de se diriger dans une ville, devant faire appel à sa femme sitôt le premier coin de rue franchi. Cela ne l'handicapait pas cependant pour travailler dans des espaces de dimension infinie.

Schwartz a été Professeur à Polytechnique, y créant à partir de rien un grand centre de recherche mathématique. Il est à l'origine d'une grande partie de l'école française d'analyse actuelle.

Atle Selberg (Norvège, 1917-)

pour ses résultats sur la conjecture de Riemann et pour avoir donné, de l'équivalence, lorsque n tend vers l'infini, entre $n/\ln n$ et le nombre $\pi(n)$ de nombres premiers $\leqslant n$), une démonstration élémentaire dont on s'était demandé pendant 50 ans si elle existait ou non. Ce résultat avait été conjecturé avant 1800 par Gauss et, indépendamment, par Legendre ; il n'avait été démontré qu'en 1896 par Hadamard et de la Vallée Poussin ; leur démonstration utilisait les fonctions de variable complexe.

1954

Kunihiko Kodaira (Japon, 1915-1997)

pour ses travaux sur les intégrales harmoniques et leurs applications aux variétés kählériennes.

Jean-Pierre Serre (France, né en 1926

Jean-Pierre Serre est le fils d'un pharmacien ; il est né dans les Pyrénées-Orientales. Après l'École Normale supérieure, il écrit rapidement une thèse splendide sous la direction d'Henri Cartan en développant des techniques dues à Leray pour calculer des objets de la topologie algébrique, en particulier les groupes d'homotopie des sphères. Il en est récompensé par une médaille Fields en 1954, à 28 ans, un record. Dès 1956, il est nommé professeur au Collège de France. Il le restera jusqu'à sa retraite, en 1994, respectant la règle de cette institution : enseigner chaque année des résultats nouveaux. Ses cours le conduisent à écrire une douzaine de livres, tous devenus des classiques et souvent réédités ; son *Cours d'arithmétique* est un vrai succès. Ses œuvres complètes forment quatre épais volumes. Le style de Serre est la perfection de la rédaction, concise, précise et élégante. Ses travaux ont marqué des branches entières de l'algèbre et de la géométrie actuelle et sont constamment utilisés. Citons *Faisceaux algébriques cohérents* de 1955 où il introduit des méthodes cohomologiques en géométrie algébrique, et *Géométrie algébrique et géométrie analytique*, de 1956, connu par ses initiales : GAGA, ceux de théorie des nombres, sur les courbes elliptiques, etc.

Serre a été le premier lauréat du Prix Abel en 2003 pour *son rôle central dans l'élaboration de la forme moderne de nombreux domaines des mathématiques,*

notamment la topologie, la géométrie algébrique et la théorie des nombres.

Un extrait d'une entrevue en anglais. À la question : *How important is inspiration in the discovery of theorems ?*, Serre répond :

I don't know what "inspiration" really means. Theorems, and theories, come up in funny ways. Sometimes, you are just not satisfied with existing proofs, and you look for better ones, which can be applied in different situations. A typical example for me was when I worked on the Riemann-Roch theorem (circa 1953), which I viewed as an "Euler-Poincare" formula (I did not know then that Kodaira-Spencer had had the same idea.) My first objective was to prove it for algebraic curves - a case which was known for about a century ! But I wanted a proof in a special style ; and when I managed to find it, I remember it did not take me more than a minute or two to go from there to the 2-dimensional case (which had just been done by Kodaira). Six months later, the full result was established by Hirzebruch, and published in his well-known Habilitationsschrift.

Quite often, you don't really try to solve a specific question by a head-on attack. Rather you have some ideas in mind, which you feel should be useful, but you don't know exactly for what they are useful. So, you look around, and try to apply them. It's like having a bunch of keys, and trying them on several doors.

1958

Klaus Roth (Angleterre, 1925-)

pour ses travaux de théorie des nombres, en particulier le résultat suivant : si a est un nombre algébrique irrationnel et k un nombre réel tel qu'il existe une infinité de nombres rationnels tels que : $|a - p/q| < 1/q^k$, alors $k \leqslant 2$.

René Thom (France, 1923-2002)

pour ses travaux en géométrie différentielle : création de la théorie du cobordisme, contenant en germe sa théorie des catastrophes qui l'a, depuis une vingtaine d'années, rendu célèbre.

1962

Lars Hormander (Suède, 1931-)

pour ses travaux sur les équations aux dérivées partielles réputés extraordinairement novateurs.

John Milnor (Etats-Unis, 1931-)

pour ses travaux en topologie différentielle, en particulier la découverte surprenante de nouvelles structures sur des sphères telles que celles de $\mathbb{R}^8$.

1966

Michael Atiyah (Angleterre, 1929-)

pour ses travaux en K-théorie, sur le théorème de l'indice et des formules de point fixe.

Paul Cohen (Etats-Unis, 1934-)

pour avoir établi l'indépendance de l'hypothèse du continu (problème de théorie des ensembles posé en 1878 par Cantor et classé npar Hilbert en 1900 dans sa célèbre série de problèmes) en créant la méthode du forcing.

Alexandre Grothendieck (France, 1928-)

Le père de Grothendieck a été longuement engagé dans des combats révolutionnaires jusqu'à sa mort en 1942, dans un camp. Grothendieck passe alors deux ans au Chambon-sur-Lignon, la célèbre commune des Cévennes où 3 à 5000 enfants juifs furent sauvés par la population huguenote et le pasteur André Trocmé (1905-1971). Il étudie à Montpellier, travaillant seul, passe une année par Paris et apparaît dans le monde mathématique à Nancy en 1951, où il va voir Dieudonné et Schwartz. Il a des idées très générales (trop, lui dit Dieudonné, très agacé). Ils lui donnent une liste de 14 questions auxquelles ni l'un ni l'autre ne savent répondre ; Grothendieck disparaît ; quelques semaines plus tard, il revient avec des solutions *profondes et difficiles*, écrit Schwartz.

Apatride, refusant de faire son service militaire pour être naturalisé français, Grothendieck ne peut trouver de poste après sa thèse et part à l'étranger. Quand il revient, il s'oriente vers la géométrie algébrique. Il est nommé professeur dans un Institut nouvellement créé : l'IHES (Institut des hautes études scientifiques) construit à Bures-sur-Yvette au sud de Paris dans un cadre merveilleux. Il fonde la *théorie des schémas*, une révolution dans la géométrie algébrique, dans le but de démontrer les conjectures de Weil sur le nombre de solutions d'équations polynomiales à coefficients dans des corps finis. Ses discussions et ses échanges de lettres avec Serre sont essentiels. Dans ce nouveau cadre, la théorie des équations polynomiales est développée sur des anneaux et non plus seulement sur des corps, ce qui permet une unification de la géométrie algébrique et de la théorie des nombres suivant des idées de Serre, Weil et Galois. Pour Grothendieck : *on n'attaque pas de front un problème, mais on l'enveloppe et le dissout dans une marée montante de théories générales.*

Les publications de Grothendieck des années 1960-1970, avec l'aide de Dieudonné, forment un ensemble extraordinaire de plusieurs milliers de pages ; elles ont engendré des centaines de travaux. Le mardi était une journée chargée : cours de Serre au Collège de France le matin, déplacement dans la vallée de Chevreuse le midi, séminaire de l'IHES l'après-midi ; Serre et Grothendieck se voyaient à cette occasion ; leurs approches se complétaient, Serre étant toujours prudent, Grothendieck lançant sans cesse de nouvelles idées (voir *Correspondance Grothendieck-Serre*, SMF, 2001). Tous ceux qui l'ont vécu s'en souviennent comme d'une période unique dans leur vie.

Grothendieck a reçu la médaille Fields en 1966 sans aller la chercher à Moscou. À partir de 1970, il change de vie. Toujours avec la même énergie, il devient militant écologiste, fonde son propre mouvement. Il abandonne (au moins apparemment) les mathématiques pendant quelques années. Il y revient dix ans plus tard : *La longue marche à travers la théorie de Galois* (1980-1981, 1600 pages manuscrites), *Esquisse d'un programme* (de candidature à un poste au CNRS, dont les 48 pages contiennent des merveilles comme ce qu'on appelle les *dessins d'enfants* qui permet des représentations de l'un des objets les plus fascinants : le groupe de Galois de $\bar{\mathbb{Q}}$ (corps des nombres algébriques) sur $\mathbb{Q}$.

Au milieu des années 1980, Grothendieck publie un très long texte autobiographique : *Récoltes et semailles*, qu'on peut trouver sur la Toile. Dans une très belle langue, Grothendieck cherche à analyser ses relations avec les mathématiques, avec ses collègues, avec lui-même, donnant à lire ses inter-

rogations, ses doutes et ses idées jour après jour.

Grothendieck a coupé depuis peu à peu ses relations avec le monde ; il vit dans les Pyrénées, demandant la préservation de sa tranquillité.

Stephen Smale (Etats-Unis, 1930-)

pour avoir démontré pour $n \geqslant 5$ l'hypothèse de Henri Poincaré : en 1904, Poincaré avait posé le problème de savoir si, comme il l'avait démontré pour n égal à 1 et 2, toute surface ayant certaines propriétés de la sphère de dimension n pouvait être déformée en cette sphère. S. Smale a aussi beaucoup développé les études de stabilité dans les systèmes différentiels.

1970

Alan Baker (Angleterre, 1939-)

pour ses travaux sur les nombres transcendants et les solutions des équations à coefficients entiers.

Heisouke Hironaka (Japon, 1931-)

pour un théorème très puissant, réputé de démonstration extrêmement difficile en géométrie algébrique sur la résolution des singularités.

Serguei Novikov (Urss, 1938-)

pour ses travaux en topologie différentielle.

John Thomson (Etats-Unis, 1932-)

pour ses travaux pour la détermination des groupes finis simples, travail commencé par Evariste Galois en 1830 et qui devait être achevé (du moins le crut-on) en 1982.

1974

Enrico Bombieri (Italie, 1940-)

pour ses travaux sur la distribution des nombres premiers (étudiés depuis Dirichlet en 1837), en analyse sur la conjecture de Bieberbach et en géométrie algébrique.

David Mumford (Etats-Unis, 1937-)

pour ses travaux en géométrie algébrique.

1978

Pierre Deligne (Belgique, 1944-)

pour la démonstration des conjectures d'André Weil, datant de 1949, sur le nombre de solution de certaines équations, en utilisant les résultats de la théorie des schémas d'Alexandre Grothendieck.

Charles Feffermann (Etats-Unis, 1949-)

pour ses travaux sur les équations différentielles.

Gregori Margoulis (Urss, 1946-)

pour ses travaux en théorie des groupes algébriques.

Daniel Quillen (Etats-Unis, 1940-)

pour ses travaux de topologie algébrique.

1982

Le congrès des mathématiciens, qui devait se réunir à Varsovie en 1982, avait dû être reporté d'un an à cause des difficultés que connaissaient les mathématiciens polonais avec le pouvoir communiste.

Alain Connes (France, 1947-)

Certains mathématiciens ont un esprit d'une grande rapidité, comprenant tout instantanément. Alain Connes dit ne pas être de ceux-là ; il n'est pas le premier arrivé au pied du mur, mais il a des qualités que d'autres n'ont pas pour le franchir. Le sujet de sa thèse est la classification d'algèbres d'opérateurs, sujet de recherche ouvert par Von Neumann et dans lequel Connes obtient de nombreux résultats qui lui valent la médaille Fields en 1983. Connes est professeur au Collège de France depuis 1984. Il cherche à unifier la relativité générale et la mécanique théorique en développant dans les années 1980 les outils et les concepts de la *géométrie non commutative*. Dans ce cadre, les idées de symétrie de Galois et les travaux de Grothendieck ouvrent vers de nouveaux horizons sur la géométrie de l'espace-temps que Connes continue à explorer... Ce travail pour la connaissance et la compréhension profonde de notre monde est essentiel, même s'il est sans doute sans applications immédiates.

William Thurston (Etats-Unis, 1946-)

Thurston est décidé dès l'âge de 8 ans à devenir mathématicien. À 21 ans, il part travailler en Californie, à Berkeley, avec, notamment, Stephen Smale, Médaille Fields 1966.

Ses travaux des années 1970 sur la géométrie des surfaces de dimension 3 révolutionnent un domaine des mathématiques abordé par Poincaré. Il crée des outils nouveaux et obtient des résultats surprenants qui lui valent la médaille Fields en 1982-83. Les surfaces de dimension 2 peuvent ressembler, localement, à une surface plane, une surface ronde comme la sphère ou une surface plissée comme le plan hyperbolique. La grande conjecture de Thurston est que les surfaces de dimension 3 auraient toutes, en un certain sens, une géométrie ; ces géométries seraient de huit types différents. L'un de ces types est celui de la sphère de dimension 3 (d'équation $x^2 + y^2 + z^2 + t^2 = 1$ dans l'espace de dimension 4) et le problème de Thurston dans ce cas se ramène à la conjecture de Poincaré démontrée par Perelman.

Les idées de Thurston se sont révélées extrêmement fécondes et de nombreux mathématiciens travaillent sur les multiples aspects de sa conjecture. Il achète au marché de Sacramento en Californie des légumes et des fruits de toutes formes, des feuilles de moutarde avec leurs replis, etc. pour expliquer à ses étudiants la géométrie des surfaces ; il veut développer l'intuition, le

formalisme mathématique vient après.

Shing Tung Yau (Etats-Unis, 1949-)

pour ses travaux sur les équations aux dérivées partielles : résolution de la conjecture de Calabi, équation de Monge-Ampère...

1986

Simon Donaldson (Angleterre, 1957-)

pour ses travaux de géométrie différentielle en dimension 4, qui ouvrent des voies entièrement nouvelles.

Gerd Faltings (Allemagne, 1954-)

pour la résolution de la conjecture faite par Mordell en 1922 : il n'existe qu'un nombre fini de solutions rationnelles d'une équation polynomiale à coefficients entiers ; lui aussi utilise les résultats de la théorie des schémas crée par Alexandre Grothendieck.

Michael Friedman (Etats-Unis)

pour avoir résolu la conjecture de Poincaré pour $n = 4$ en classifiant toutes les surfaces de dimension 4.

1990

V. G. Drinfeld (Russie, 1954-)

pour ses travaux sur la correspondance de Langlands entre certaines représentations de groupes de Galois de corps de fonctions et des formes automorphes et d'autres travaux sur les groupes quantiques.

Vaughan Jones (Nouvelle Zélande, 1952-)

pour ses résultats sur la classification des algèbres de Von Neumann laquelle a des applications inattendues et fructueuses, par exemple en permet-

tant de calculer de nouveaux invariants polynomiaux en théorie des nœuds, sources de nouvelles idées.

Shigefumi Mori (Japon, 1951-)

pour ses travaux sur la géométrie des variétés algébriques complexes, en particulier en dimension 3.

Edward Witten (Australie, 1951-)

pour la fertilité exceptionnelle de son approche des mathématiques à partir de sa spécialité : la théorie des particules élémentaires, renouvelant la théorie de Morse, la théorie de Atyah-Singer, théories elliptiques en cohomologie, etc.

1994

Jean Bourgain (Belgique, 1954-)

pour ses résultats d'analyse fonctionnelle obtenus par une approche probabiliste.

Pierre-Louis Lions (France, 1956-)

pour ses nombreux résultats sur des équations aux dérivées partielles de la physique, théorème d'existence de solutions pour le modèle de Boltzmann, étude des solutions d'équations, etc.

Jean-Christophe Yoccoz (France, 1957-)

Jean-Christophe Yoccoz étudie les systèmes dynamiques, théorie initiée par Poincaré dans son étude du système solaire (voir p. **??**).

Poincaré avait commencé à étudier un système dynamique particulier, appliquant aux points d'un cercle un très grand nombre de fois la même application. Quel est le résultat global : proche d'une rotation (en un certain sens) ou non ? Cela dépend, comme l'ont montré Herman et Yoccoz, de propriétés fines de la fonction. En 1994, Yoccoz a reçu la médaille Fields. Il est maintenant professeur au Collège de France et membre de l'Académie des sciences. Il a dit de ses travaux : *Je suis incapable de décrire les applications*

éventuelles de mes recherches à des domaines précis ni de prévoir de quelle manière, dans dix ans, mes résultats auront été utilisés. Mais il existe peu de domaines des mathématiques qui, à un moment ou un autre, ne soient applicables.

Efim Zelmanov (Russie, 1955-)

pour ses résultats sur le problème de Burnside en théorie des groupes.

1998

Maxime Kontsevitch (Russie, 1964-)

spécialiste de la théorie des cordes, de la théorie des champs quantiques et de la théorie des nœuds, travaillant actuellement à l'Institut des Hautes Etudes Scientifiques (IHES) à Bures sur Yvette depuis 1995.

Curtis McMullen (Etats-Unis, 1958-)

pour ses travaux reliant les objets géométriques de dimension 3 et les états de transition d'un régime régulier à un régime chaotique en physique.

Physicists have found a surprising amount of common structure in different systems whose behavior changes from predictable to unpredictable. Examples include smoothly flowing water that becomes turbulent, asteroids suddenly swinging out of regular orbits, and a heart suddenly starting to beat irregularly. McMullen has constructed a new geometric perspective on the structures common to such physical changes.

There are many practical applications to this work, *he said*, such as more detailed knowledge of how heart attacks begin, how earthquakes start, and how an asteroid might suddenly change its path and head for Earth.

Richard Borcherds (Angleterre, 1959-)

pour la démonstration de la conjecture Moonshine, formulée par John Conway et Simon Norton dans les années 1970 et liant le groupe appelé le monstre et les fonctions elliptiques.

Timothy Gowers (Angleterre, 1963-)

pour ses recherches en analyse fonctionnelle dans lesquelles il utilise l'analyse combinatoire de manière surprenante, démontre des conjectures de Banach, etc.

2002

Laurent Lafforgue (France, 1966-)

pour la démonstration de la conjecture de Langlands dans un cas très général. Cette conjecture relie des partie de la théorie des nombres, de l'algèbre et de l'analyse. Elle a été énoncée par le mathématicien canadien Robert Langlands en 1967 (au départ, dans une lettre fameuse à André Weil).

Vladimir Voevodski (Russie, 1966-)

pour avoir développé de nouvelles théories cohomologiques pour les variétés algébriques.

2006

Wendelin Werner (né en 1968)

Actuellement professeur à Orsay, Wendelin Werner a été élève de l'Ecole normale supérieure de la rue d'Ulm à Paris, lieu d'excellence pour la formation mathématique en France, par où sont passés les autres médaillés français. *La physique n'est pas ma motivation première, mais elle me fournit de beaux objets et de beaux problèmes mathématiques,* dit Wendelin Werner. Elle l'a mené à se poser des problèmes sur les mouvements aléatoires comme le mouvement brownien, à définir des probabilités de leur forme, de leur dimension fractale, de leurs intersections. Il dit qu'il va maintenant s'attaquer à résoudre des conjectures non encore résolues dans ces domaines.

Voici un problème résolu par Wendelin Werner. On considère des particules pouvant se déplacer par saut d'un point à coordonnées entières du plan à un de ses quatre voisins à coordonnées entières, les probablités de déplacement sur chacun de ces quatre points étant égales à 1/4. Wendelin Werner a montré une formule conjecturée en 1988 par des physiciens donnant

la probabilité qu'ont deux particules, partant d'un point donné, de se rencontrer à nouveau en moins de n déplacements. Wendelin Werner a également montré une conjecture faite par Benoît Mandelbrojt en 1982, sur la dimension fractale de la frontière de la trajectoire d'une particule soumise à un mouvement brownien : elle est de $4/3$; il a retrouvé cette même constante dans des problèmes de percolation. Les démonstrations sont évidemment très difficiles et utilisent des outils mathématiques mis au point ces dernières années. On trouve sur Internet de nombreux sites complétant ces informations.

Grigori Perelman (Russie, né en 1966)

Perrelman est célèbre pour avoir résolu la conjecture de Poincaré et pour avoir refusé la médaille, geste qui intéresse plus les journalistes qu'un résultat mathématique. Il est resté tranquillement auprès de sa famille continuer à faire ce qui l'intéresse.

Andrei Okounkov (Russie, né en 1969)

Andrei Okounkov est né en 1969 et a fait ses études à Moscou. C'est un élève d'Alexandre Kirillov (né en 1936), lui-même élève d'Israil Gelfand (né en 1913), ce dernier étant élève d'Andrei Kolmogorov (1903-1987). Andrei Okounkov a poursuivi les thèmes de recherche abordés par cette lignée de très grands mathématiciens : théorie des représentations, des groupes de Lie, etc., ses recherches le conduisant à multiplier les regards sur les problèmes qu'il étudie en mettant en œuvre des idées venant de domaines variés, aussi bien de la théorie des probabilités que de la géométrie algébrique ou de la physique mathématique.

Andrei Okounkov est depuis 2002 professeur à l'Université de Princeton, un des hauts lieux de la recherche mathématique, à deux heures de train de Manhattan. Il a reçu une médaille Fields des mains du roi d'Espagne le 22 août 2006, comme les autres médaillés de 2006) pour avoir révélé des connexions nouvelles et profondes entre.différents champs des mathématiques et de la physique ouvrant de nouveaux domaines de recherches et ayant de nombreuses applications. Partons de l'un des objets d'étude d'Andrei Okounkov, le groupe S_∞ des permutations de l'ensemble des entiers naturels qui ne permutent qu'un ensemble fini d'éléments chacune. L'étude des groupes utilise leur représentation géométrique comme isométries d'un espace, ce qui est utile en mécanique quantique. Pour le groupe S_∞, Andrei Okounkov a

réussi à décrire dans sa thèse une partie de ces représentations.

Un problème lié au précédent est l'étude des partitions d'un entier n, abordée par Euler en 1748. Une partition d'un entier n est la donnée d'une suite décroissante d'entiers non nuls de somme n ; par exemple, les 11 partitions de 6 sont données par 6=6=5+1=4+2=4+1+1=3+3=3+2+1, etc. En utilisant un quart de plan quadrillé, une partition peut-être représenté par un empilement de lignes de carrés à partir des axes, les nombres de cases des lignes correspondant aux entiers d'une partition.

En normalisant les représentations des partitions à l'aide d'un facteur $1/\sqrt{n}$, chaque partition est associée à une courbe en escalier limitant une surface unité. On peut alors se poser des questions de probabilité ou de géométrie, comme : quelle est la limite des courbes en escalier, etc. Un des nombreux résultats d'Okounkov sur ce sujet montre que la courbe limite entre les parties planes et la zone de petits cubes est une droite, ce qui demande une explication : cette affirmation est bien vraie, mais du point de vue de ce qu'on appelle la géométrie tropicale.

Terence Tao (Australie, né en 1975)

Il a obtenu une médaille de bronze aux Olympiades de mathématiques à l'âge de 11 ans, une médaille d'argent à 12 ans et une médaille d'or à 13 ans (personne n'a jamais fait aussi bien !).

Nombre de médailles par pays de 1932 à 2002

Etats-Unis 12
France 9
Angleterre 6
Urss, Russie, Ukraine 8
Japon 3
Belgique 2
Allemagne 1
Australie 2
Finlande 1
Italie 1

Norvège 1
Nouvelle Zélande 1
Suède 1

7.3 John Forbes Nash (né en 1928)

John Nash naît à Bluefield, en Virginie occidentale. Son père a des connaissances en électricité et sa mère en langues. John semble s'ennuyer en classe, ses relations avec les enfants de son âge sont un peu bizarres. Vers 12-14 ans, il pense devenir ingénieur électricien, fabrique des montages astucieux. Puis il se tourne vers les mathématiques au Carnegie Institute de Pittsburg ; sa culture mathématique s'étend rapidement ; il a du goût pour les problèmes difficiles, ses idées sont très originales. Il est recruté à Princeton par Solomon Lefschetz ; il y retrouve de très grands savants : Artin, Einstein, Gödel, Von Neumann, etc.

Le livre de théorie des jeux de Von Neumann et Morgenstern datait de 1944 ; il montrait comment modéliser différentes parties de l'économie en considérant des jeux que Nash appelle coopératifs, où les joueurs pouvaient conclure des accords avec d'autres joueurs. Nash va aller beaucoup plus loin. Il envisage des jeux non coopératifs où les joueurs élaborent leur stratégie dans le but de maximiser leurs gains, chaque joueur étant censé tout connaître de l'état de la situation et des stratégies des autres joueurs et choisissant les meilleures actions possibles (les actions sont évaluées par des fonctions d'utilité). En quelques pages, Nash montre que ces jeux possèdent des points d'équilibre (appelé équilibres de Nash) correspondants à des points fixes et dont il n'est pas avantageux de s'écarter. L'intérêt des résultats de Nash n'a pas été immédiatement compris et il a fallu du temps pour découvrir qu'ils pouvaient s'appliquer à des problèmes très variés, aussi bien ceux de l'économie de marché (travaux d'Arrow et Debreu sur les équilibres en concurrence parfaite) que ceux de la biologie et bien d'autres.

Ce sont ces travaux qui valent aujourd'hui sa célébrité à John Nash. Ce sont eux qui lui ont valu le prix Nobel d'économie en 1994.

Cependant, il ne faut pas oublier que Nash produisit au début des années 1950 des résultats exceptionnels sur les variétés algébriques réelles et riemaniennes qui lui promettaient la médaille Fields.

C'est alors que les comportements bizarres et insupportables de Nash évoluent rapidement en 1958 vers des bouffées délirantes annonciatrices d'une

terrible maladie. La schizophrénie submerge Nash pendant de longues années et c'est presque un miracle qu'elle lui ait permis, depuis une vingtaine d'années, de reprendre des activités de recherche. Ceux qui veulent tout savoir de l'histoire de la maladie de Nash liront le livre *Un cerveau d'exception* dont on a tiré en 2001 le film *Un homme d'exception*.

7.4 La création du prix Abel

En 2003, les Norvégiens ont fondé le prix Abel, avec le soutien de l'Union Mathématique Internationale. Il doit être décerné tous les ans ; les lauréats seront des mathématiciens, sans limitation d'âge. Il semble devoir combler l'absence de prix Nobel pour les mathématiques et le nom est particulièrement bien choisi ; Abel est un norvégien, magnifique mathématicien dont la vie a des aspects dramatiques émouvants et son nom est consonnant à celui de Nobel.

Le premier primé, en 2003, est Jean-Pierre Serre pour *son rôle central dans l'élaboration de la forme moderne de nombreux domaines des mathématiques, notamment la topologie, la géométrie algébrique et la théorie des nombres* (voir le site http ://www.abelprisen.no/).

En 2004, les mathématiciens Michael Atiyah (né en 1929) et Isadore Singer (né en 1924) sont récompensés pour leur théorème dont l'influence sur la topologie, la géométrie différentielle et la théorie quantique des champ est immense.

2005 : Peter Lax (né en 1926) ; 2006 : Lennart Carleson (né en 1928) ; 2007 : Srinivasa Varadhan (né en 1940) ; 2008 : Jacques Tits et John Thompson.

7.5 Prix prestigieux

La liste des lauréats de la fondation Wolf, depuis 1978, est aussi impressionnante : Gelfand, Leray, Weil, Henri Cartan, Kolmogorov, Gromov, etc.

D'autres prix prestigieux existent, comme le prix Nevanlinna créé par l'Université d'Helsinki récompensant tous les 4 ans depuis 1982 des travaux de mathématiques appliquées.

7.6 Les problèmes de la fondation Clay

L'homme d'affaires Landon Clay a prévu en 2000 de récompenser par un million de dollars ceux qui résoudraient l'une des sept conjectures suivantes, choisies par de grands mathématiciens actuels.

1) L'hypothèse de Riemann, qu'Hilbert avait déjà inclus dans la liste de ses 23 problèmes.

2) La conjecture de Poincaré, démontrée depuis par Perelman, qui a refusé aussi ce prix.

3) Le problème P=NP de la théorie de la complexité des algorithmes.

4) La conjecture de Hodge (1903-1975) en géométrie algébrique.

5) La conjecture de Birch (né en 1931) et Swinnerton-Dyer (né en 1927) en théorie des nombres.

6) L'étude des équations de Navier-Stokes de la mécanique des fluides (voir p. **??**).

7) L'étude des équations de Yang (né en 1922) et Mills (1927-1999) de la physique des particules.

7.7 Le jeu des très grands

C'est un jeu assez vain, mais tout le monde peut s'y amuser. Voici 18 noms :

Archimède, Euler, Gauss, Abel, Riemann, Hilbert, Von Neumann, Weyl, Kolmogorov ; du côté français : Fermat, Pascal, Lagrange, Galois, Poincaré, Leray, Weil, Serre ; et Grothendieck.

Pour des mathématiciens plus récents, l'avenir décidera.

Chapitre 8

Représentation en perspective

Je n'ai pas rédigé ce chapitre. Vous pouvez consulter le superbe livre de Daniel Arasse sur la perspective italienne, par exemple à la BU de Rennes 2 à Villejean, côte W 759.5/42.

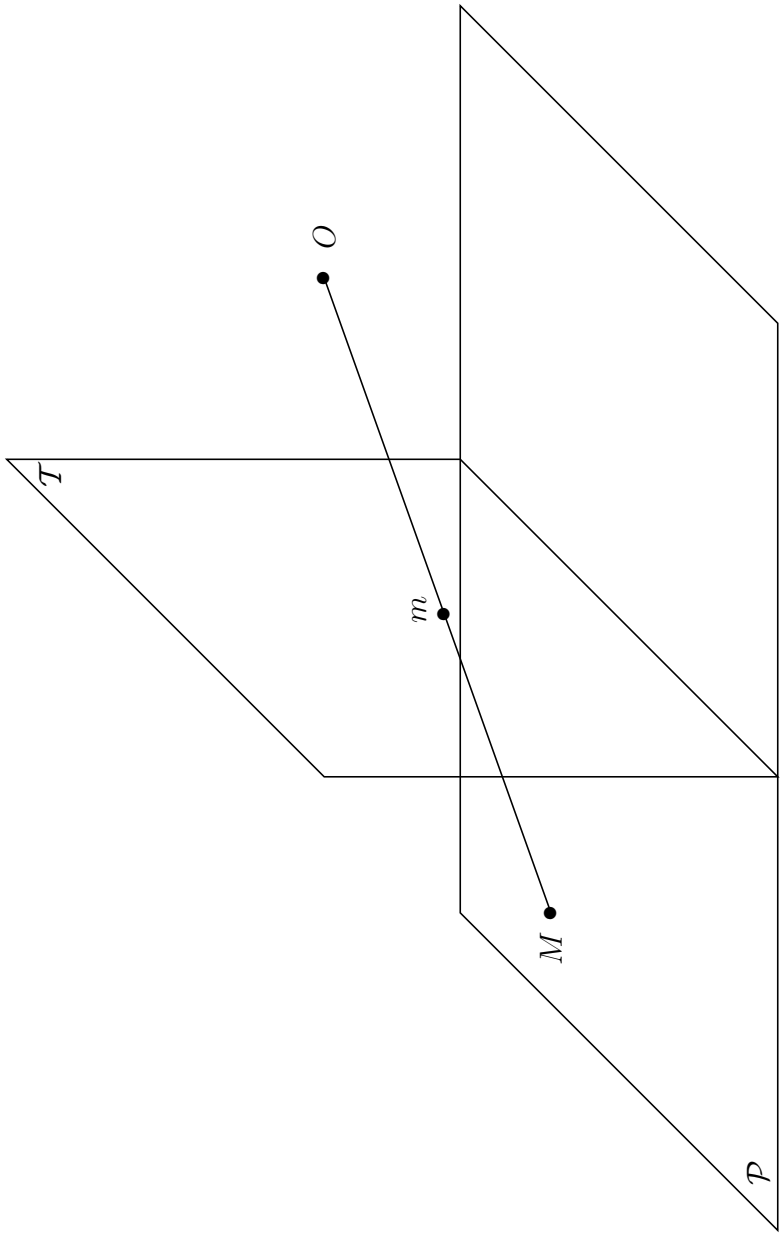


Figure 1. Image m d'un point M du plan $\mathcal{P}$ comme intersection d'une droite et d'un plan.

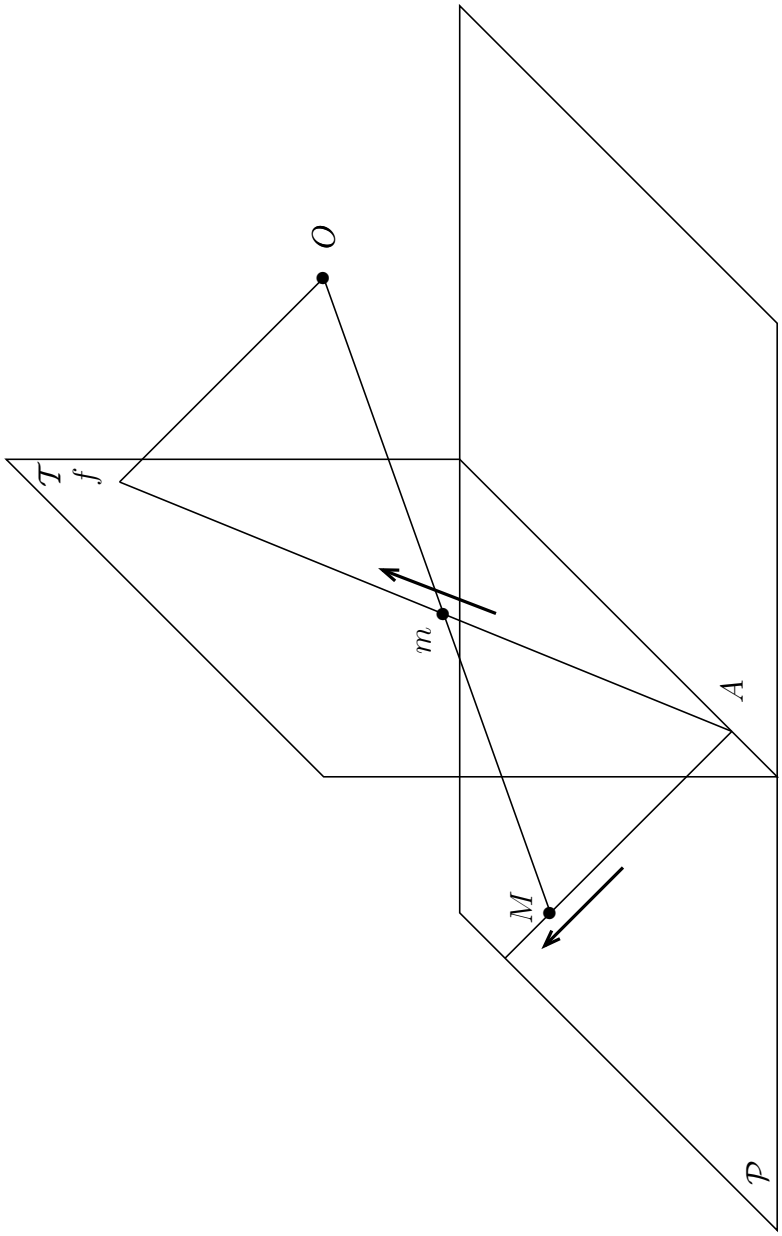


Figure 2. Image $[Af[$ de la demi-droite $[AM)$ du plan $\mathcal{P}$.

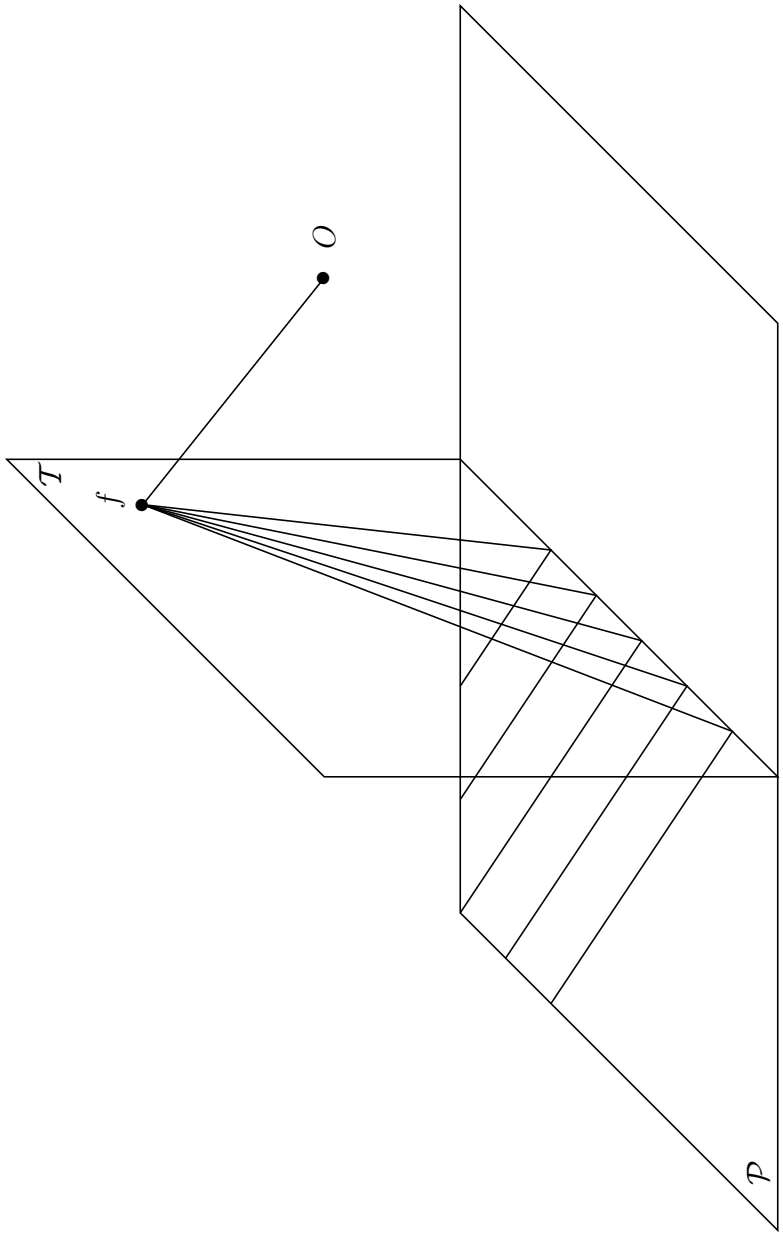


Figure 3. Image des parallèles à la demi-droite $[AM)$ du plan $\mathcal{P}$.

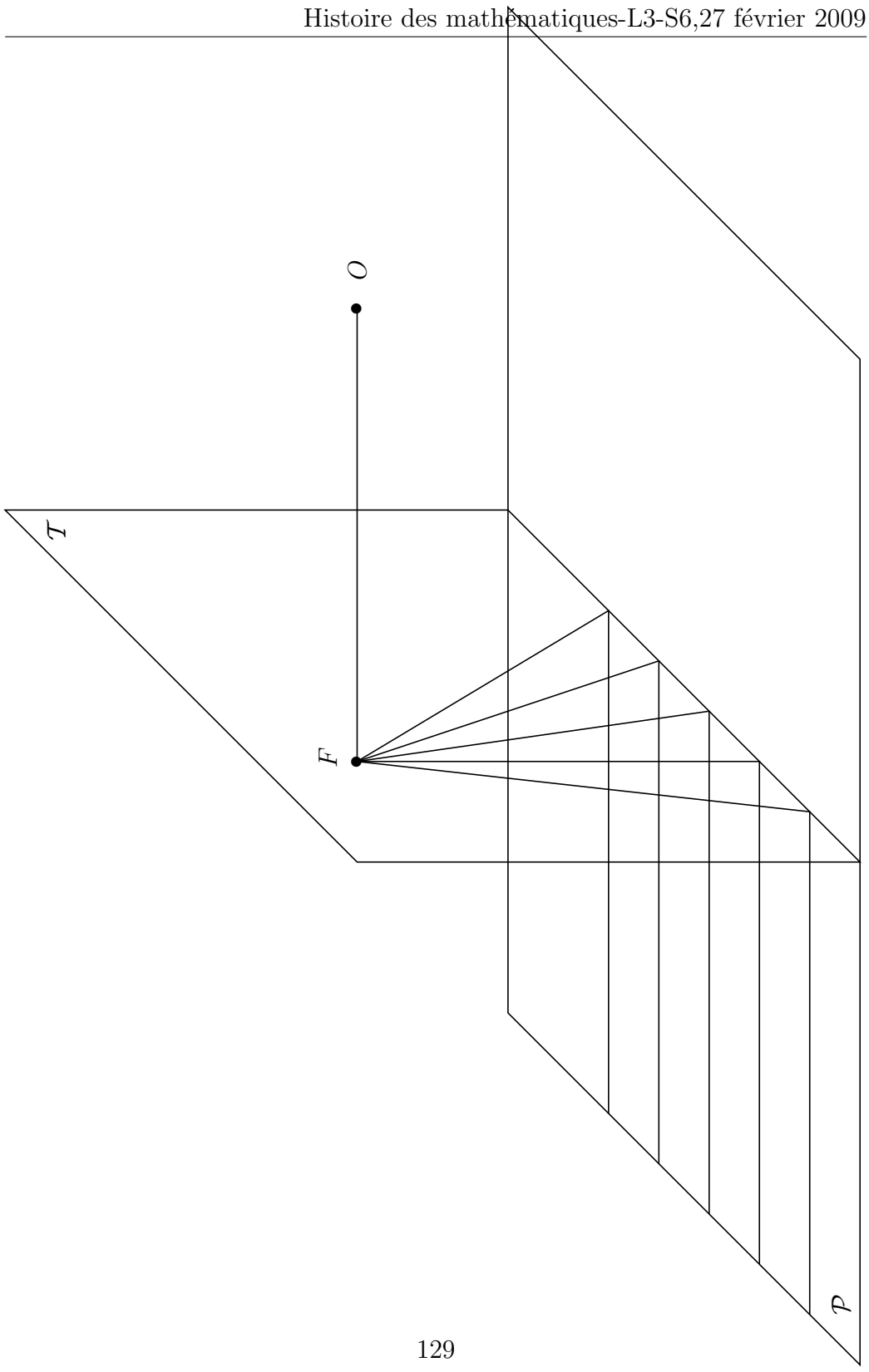


Figure 4. Image d'un parquet du plan $\mathcal{P}$ perpendiculaire au plan du tableau.

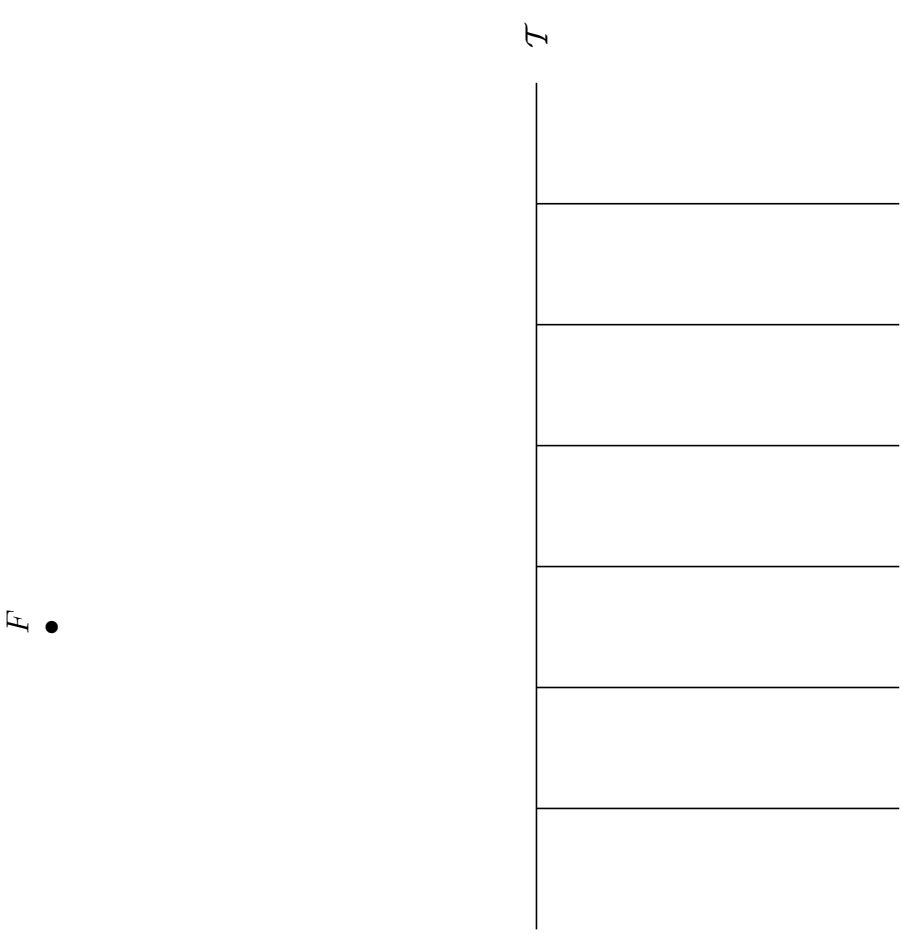


Figure 5. Exercice : image d'un parquet du plan $\mathcal{P}$ perpendiculaire au plan du tableau $\mathcal{T}$ connaissant F.

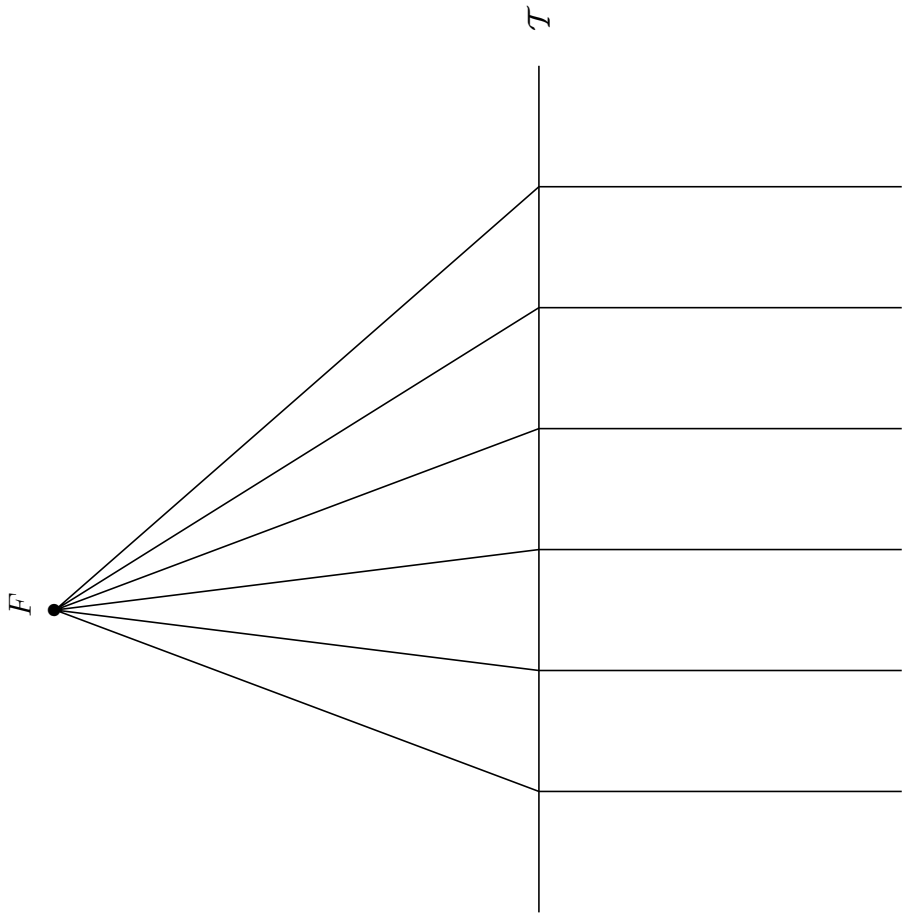


Figure 6. Image d'un parquet du plan $\mathcal{P}$ perpendiculaire au plan du tableau $\mathcal{T}$.

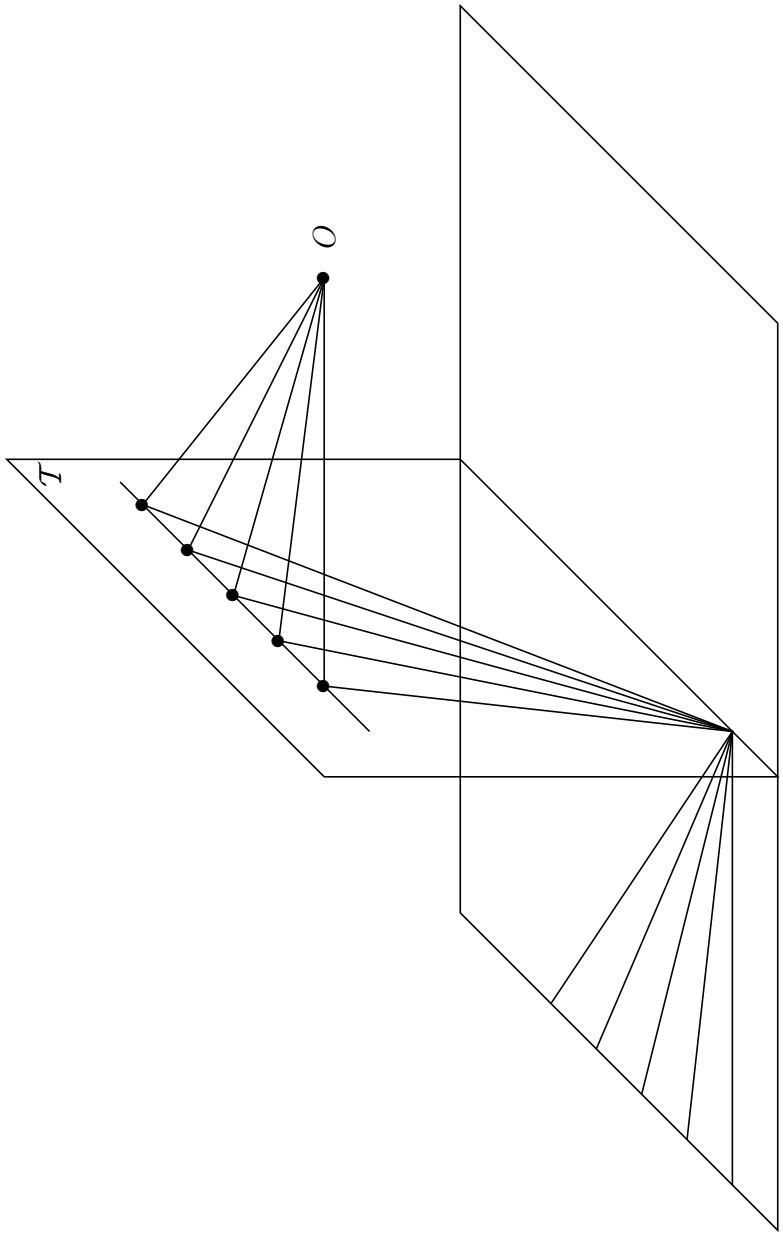


Figure 7. Alignement des points de fuite de droites du plan $\mathcal{P}$.

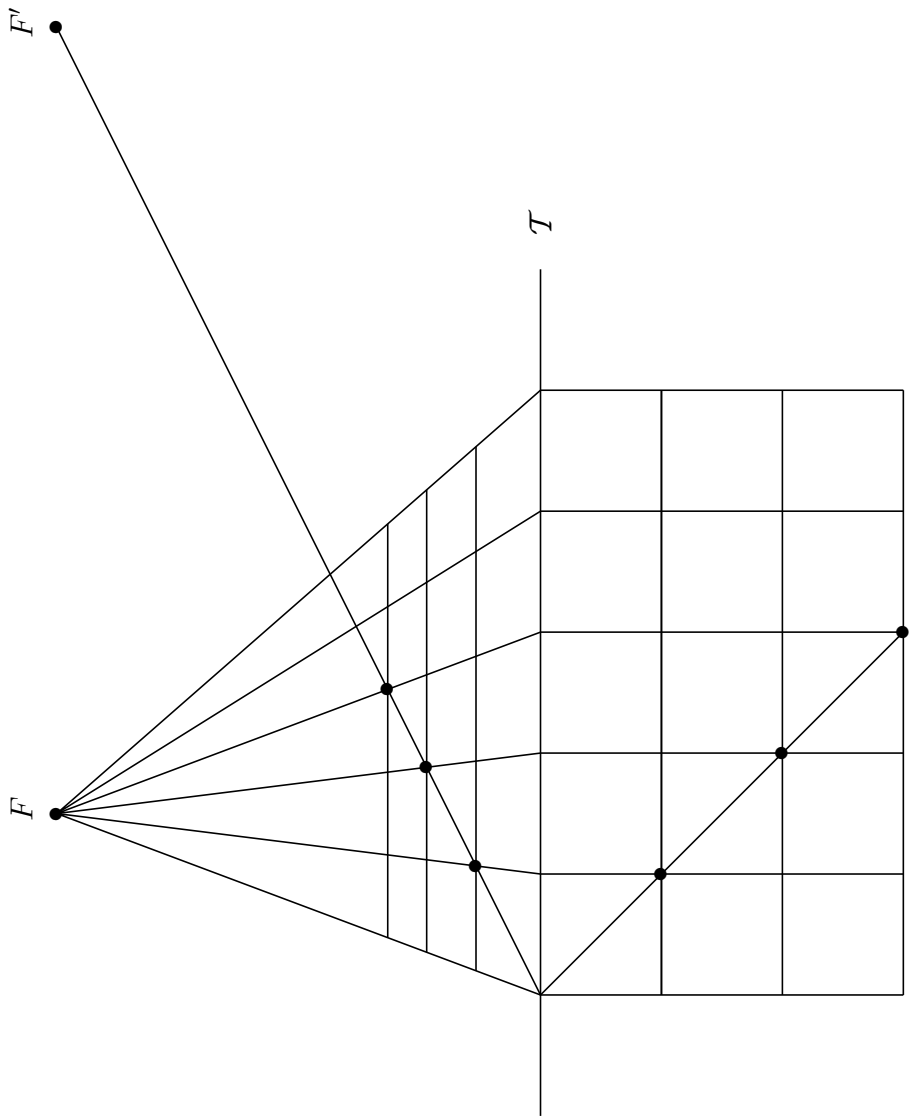


Figure 8. Image d'un carrelage du plan $\mathcal{P}$ perpendiculaire au plan du tableau $\mathcal{T}$ connaissant F et F'.

Figure 9. Exercice : construction de l'image d'un carrelage du plan $\mathcal{P}$ perpendiculaire au plan du tableau $\mathcal{T}$ connaissant les points de distance F et F'.

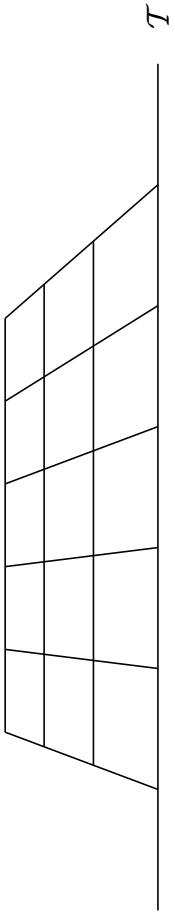


Figure 10. Exercice : détermination des points F et F' à l'aide de l'image d'un carrelage.

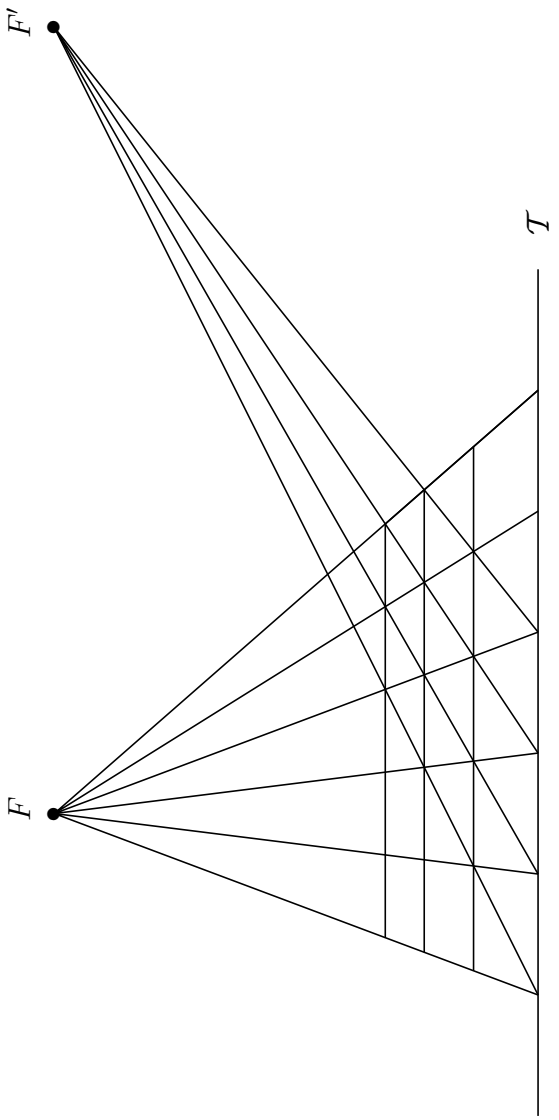


Figure 11. Détermination des points F et F' à l'aide de l'image d'un carrelage.

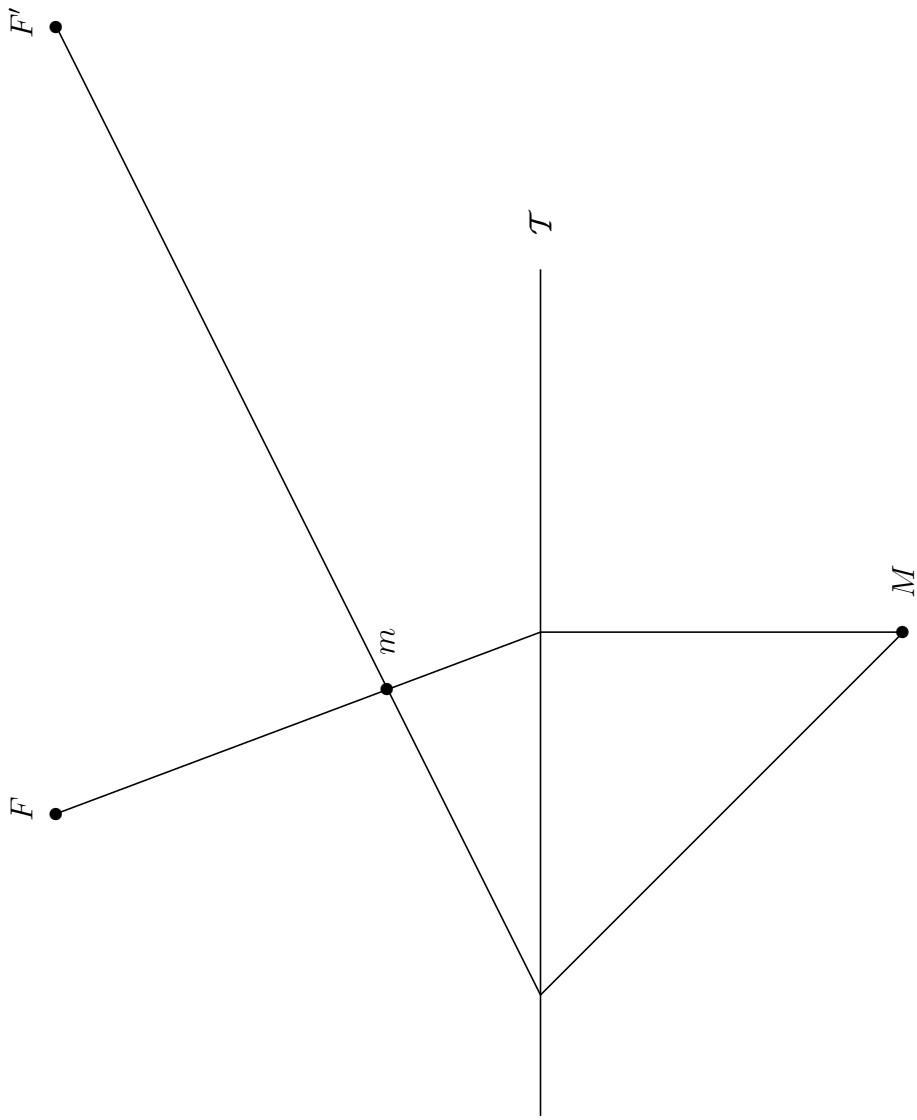


Figure 12. Construction de l'image m d'un point M du plan $\mathcal{P}$ connaissant les points de distance F et F'.

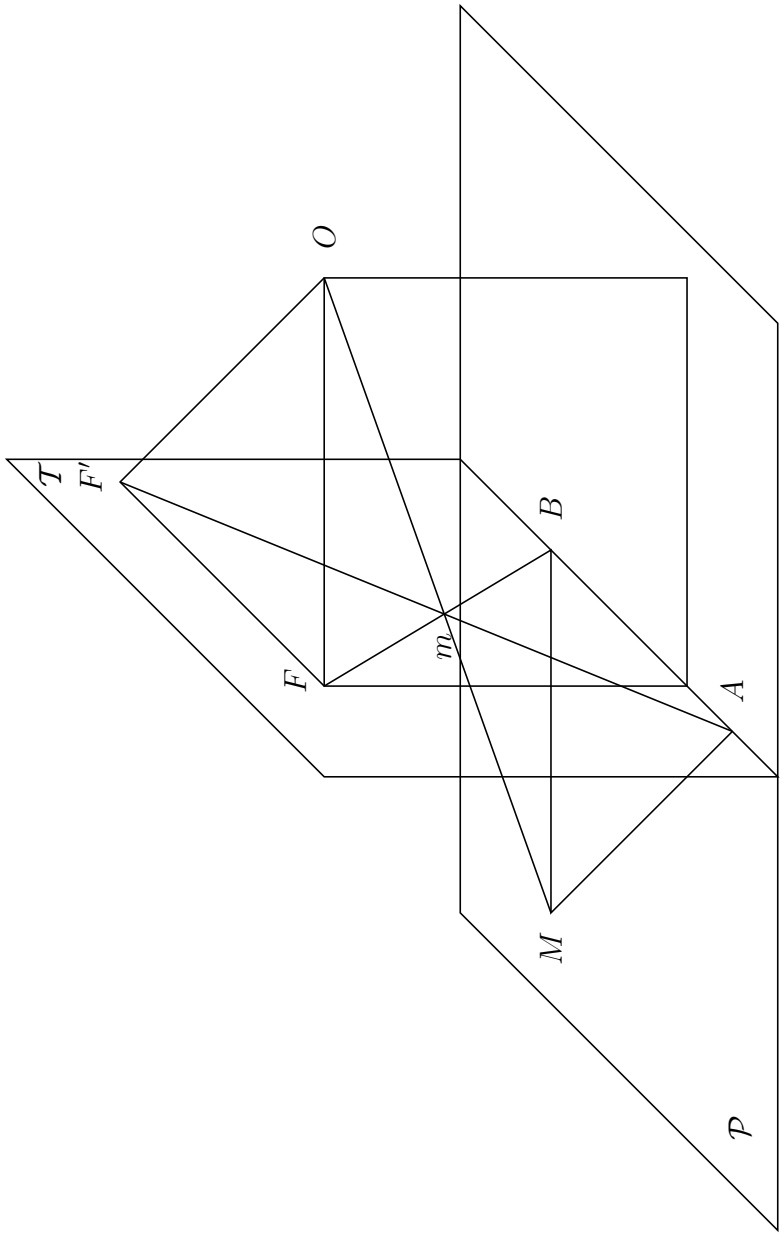


Figure 13. Construction de l'image m du point M du plan $\mathcal{P}$; O est l'œil du peintre ; $\widehat{MAB} = \widehat{FOF'} = 45°$.

Figure 14. Image d'un cercle du plan $\mathcal{P}$ connaissant les points de distance F et F'.

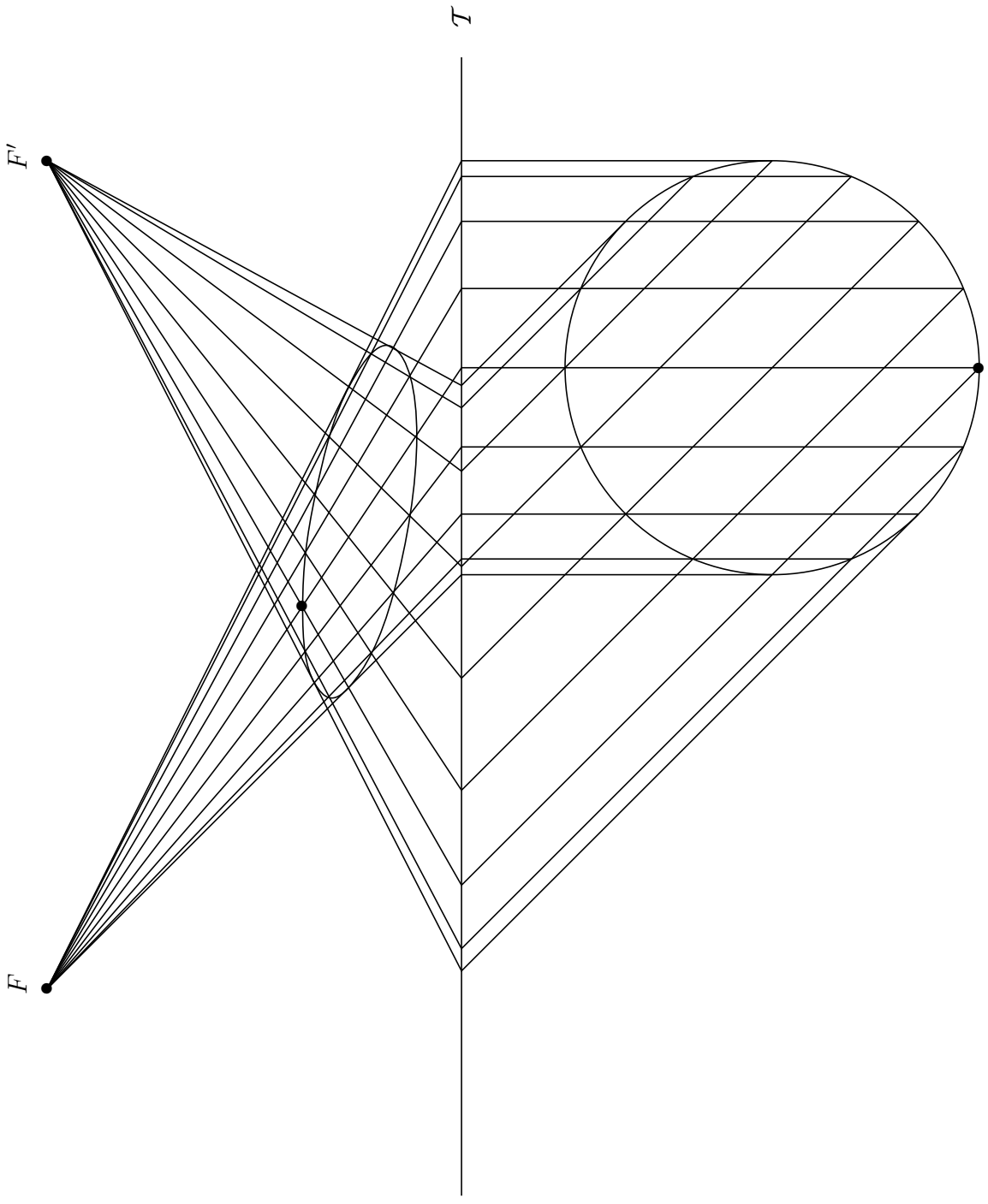


Figure 15. Image d'un cercle du plan $\mathcal{P}$ connaissant les points de distance F et F'.

Sujet d'examen

Un peintre veut représenter un motif dessiné sur le sol (voir ci-dessous) en suivant les règles de la représentation en perspective.

Son tableau est posé verticalement sur le sol. L'œil du peintre est à 1 mètre 50 du tableau et à 3 mètres au-dessus du niveau du sol ; il se projette en F sur le plan du tableau comme indiqué.

Placez un point de distance F' et représentez le tableau en utilisant le dessin suivant qu'on rendra ; on laissera les traits de construction apparents.

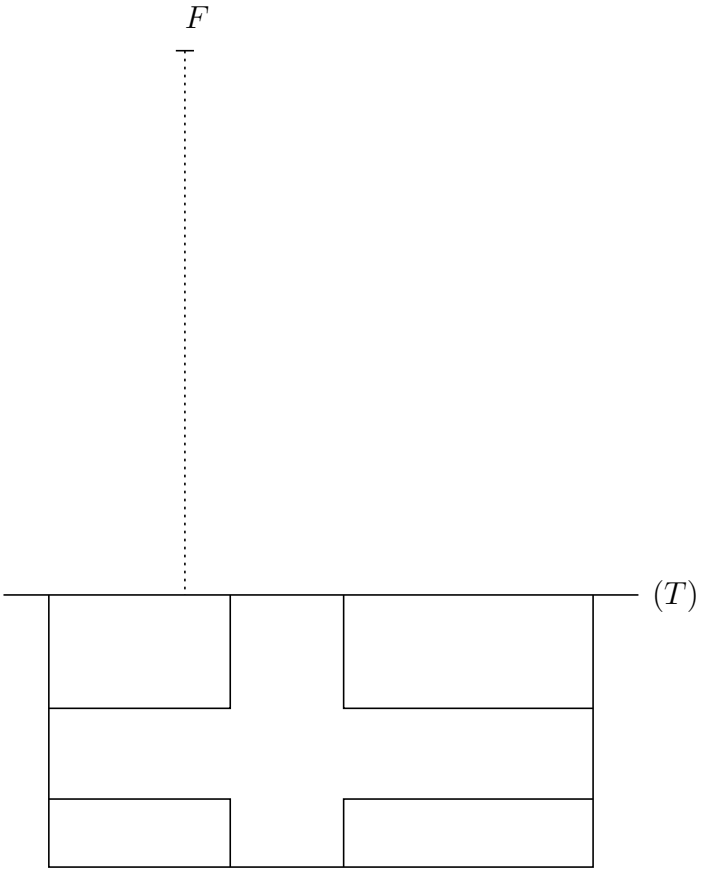


Figure 16. Sujet d'examen.

Chapitre 9

Cryptographie avant 1976

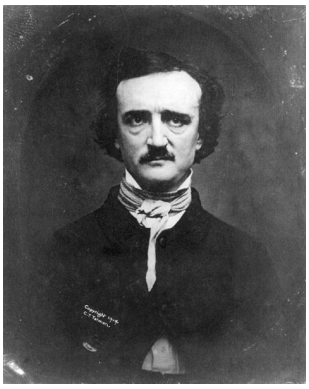
9.1 Introduction

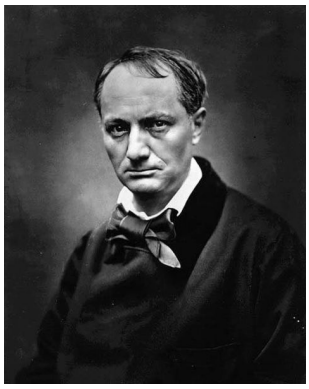
La cryptographie est, depuis plus de 2000 ans, un procédé utilisé par tout ceux qui souhaitent transmettre des informations confidentielles. Elle a pris ces deux derniers siècles une extension considérable dans les domaines militaires, diplomatiques et commerciaux. Jusqu'au milieu des années 1970, il y avait un certain équilibre entre ceux qui recherchaient les moyens les plus sûrs pour chiffrer un texte et ceux qui cherchaient à percer les secrets d'un chiffre. La situation a alors complètement changé. Les mathématiques et, particulièrement, la théorie des nombres ont trouvé des applications inattendues en cryptographie et elles semblent permettre aujourd'hui une sécurité absolue (bien qu'un tel diagnostic soit risqué, l'histoire nous montrant génération après génération, des cryptographes sûrs d'avoir trouvé un système indéchiffrable).

9.2 Le scarabée d'or

La nouvelle d'Edgar Poe (1809-1849) : *Le Scarabée d'or*, est parue les 21 et 28 juin 1843 dans le *Dollar Newspaper*, un journal de Philadelphie. Cette nouvelle raconte comment un certain William Legrand, qu'une série de malheurs a réduit à la misère, découvre par hasard sur une plage un vieux papier, en fait un vieux parchemin. Le hasard veut que Legrand passe ce parchemin devant une flamme et qu'un texte chiffré écrit à l'encre sympathique apparaisse. Dans la suite de la nouvelle, Legrand explique à un ami comment il a réussi à déchiffrer le texte. À vrai dire, le texte déchiffré est presqu'aussi

obscur que le texte chiffré et il faut toute l'ingéniosité de Legrand pour en comprendre les indications et les utiliser pour retrouver un fabuleux trésor qui devrait lui permettre de recouvrer les possessions de sa famille.





Pour lire l'histoire complète, procurez-vous les *Histoires extraordinaires* et profitez-en pour lire d'autres œuvres de Poe, comme les merveilleuses, horribles, fascinantes *Aventures d'Arthur Gordon Pym*, écrites en 1837 et publiées sans aucun succès à l'époque. Tous ces textes ont été admirablement traduits par Charles Baudelaire (1821-1867) dans les années 1850.

9.3 Le texte de l'énigme

$$53 \pm \pm + 305))6*; 4826)4 \pm .)4\pm); 8 + 6* ; 48 + 8q60))85; 1 \pm (; : \pm * 8 + 83(88)5* +; 46(; 88 * 96*?; 8) * \pm(; 485); 5 * +2 : * \pm (; 4956 * 2(5 * -4)8q8*; 4069285);)6 + 8)4 \pm \pm; 1(\pm 9; 48081; 8 : 8 \pm 1; 48 + 8 5; 4)485 + 528806 * 81(\pm 9; 48; (88; 4(\pm ?34; 48)4\pm; 161; : 188; \pm ?;$$

9.4 Le déchiffrage de l'énigme

Quand William Legrand raconte comment il a fait pour déchiffrer ce texte, il explique que la première question qui s'est posée à lui était de savoir dans quelle langue le texte originel avait été écrit. La signature du pirate

lui apprend que c'est l'anglais et non l'espagnol ou le français. Dans cette langue, selon Legrand, la lettre la plus fréquente est le e puis, dans l'ordre des fréquences décroissantes, $a\ o\ i\ d\ h\ n\ r\ s\ t\ u\ y\ c\ f\ g\ l\ m\ w\ b\ k\ p\ q\ x\ z$[1].

En fait, le e est très facile à trouver. On remarque que le texte chiffré utilise 20 caractères :

$$5\ 3\ \pm\ +\ 0\ )\ 6\ *\ ;\ 4\ 8\ 2\ .\ q\ 1\ (\ :\ 9\ ?\ -$$

et on peut établir sans difficulté le tableau des fréquences de chacun d'eux :

5	3	±	+	0	)	6	*	;	4
12	4	16	9	5	16	11	13	26	19

8	2	.	q	l	(	:	9	?	−
33	5	1	2	8	10	4	5	3	1

Ce tableau révèle sans équivoque que le e est chiffré par le 8 ; en remplaçant les 33 occurrences du 8 par des e, le texte à déchiffrer devient :

$$53\pm\pm+305))6*;4e26)4\pm.)4\pm);e+6*\\ ;4e+eq60))e5;1\pm(;:\pm*e+e3(ee)5*\\ +;46(;ee*96*?;e)*\pm(;4e5);5*+2:\\ *\pm(;4956*2(5*-4)eqe*;40692e5);\\ )6+e)4\pm\pm;1(\pm9;4e0e1;e:e\pm1;4e+e\\ 5;4)4e5+52ee06*e1(\pm9;4e;(ee;4(\\ \pm?34;4e)4\pm;161;:1ee;\pm?;$$

On vient de faire un grand pas. Legrand ne cherche pas à tirer parti des autres fréquences ; cela conduirait à des essais entre différentes lettres ; il utilise une autre particularité de l'anglais : la fréquence du mot *the*. On retrouve effectivement dans le texte chiffré huit fois le couple ;4 avant le e. Le remplacement de ; par t et de 4 par h donne, en commençant à séparer les mots (les *the*) qui semblent apparaître :

1. Des tables modernes ne donnent pas cet ordre, voir [Bauer, 1991] p. 263.

$$53 \pm \pm + 305))6 * \ the\ 26)h \pm .)h\pm)te + 6* \\ the\ + eq60))e5t1 \pm (t : \pm * e + e3(ee)5* \\ +th6(tee * 96*?te) * \pm(\ the\ 5)t5 * +2 : \\ * \pm (th956 * 2(5 * -h)eqe * h0692e5)t \\ )6 + e)h \pm \pm t1(\pm 9\ the\ 0e1te : e \pm 1\ the\ + e \\ 5th)he5 + 52ee06 * e1(\pm 9the\ t(eeth(\\ \pm ?3h\ the\ )h \pm t161t : 1eet\pm ?t$$

La suite du déchiffrage est affaire de routine ; on peut dire que le chiffrage a cédé ; il faut du travail, mais le principal a été fait.

Legrand remarque d'abord la succession *t(eeth* qui le conduit au mot *tree* (en le détachant du *th* qui suit) en supposant que la parenthèse ouvrante (chiffre le *r*. Puis la succession *the tree thr*± *?3h the* le conduit au mot *through*, donc ± chiffre le *o*, ? chiffre le *u* et 3 chiffre le *g*. On obtient :

$$5goo + g05))6 * \ the\ 26)ho.)ho)te + 6* \\ the\ + eq60))e5t1ort : o * e + egree)5* \\ +th6rtee * 96 * ute) * or\ the\ 5)t5 * +2 : \\ *orth956 * 2r5 * -h)eqe * th0692e5)t \\ )6 + e)hoot1ro9\ the\ 0e1te : eo1\ the\ + e \\ 5th)he5 + 52ee06 * e1ro9\ the\ tree\ through \\ the\ )hot161t : 1eet\ out$$

L'étape suivante consiste à deviner les mots *degree* et *thirteen*, donc +

chiffre d, 6 chiffre i et * chiffre n.

$$5\ good\ g05))\ in\ the\ 2i)ho.)ho)ted\ in\ the\ deq60))e5t1ort:\ one\ degree\ )5n\ d\ thirteen\ 9inute)*or\ the\ 5)t5*+2:\ *orth956*2r5*-h)eqe*th0692e5)t\ )6+e)hoot1ro9\ the\ 0e1te:eo1\ the\ +e\ 5th)he5+52ee06*e1ro9\ the\ tree\ through\ the\ )hot161t:1eet\ out$$

On devine alors que 5 chiffre a, ce qui donne le début du texte : *A good*, que 9 chiffre m pour former le mot *minute*, que) chiffre s pour former *degrees*, que 1 chiffre f pour former *from*, etc. Poe ne détaille pas les dernières déductions de Legrand : *Je vous en ai dit assez pour vous convaincre que des chiffres de cette nature sont faciles à résoudre, et pour vous donner un aperçu de l'analyse raisonnée qui sert à les débrouiller. Mais tenez pour certain que le spécimen que nous avons sous les yeux appartient à la catégorie la plus simple de la cryptographie.*

On aboutit au texte en anglais :

A good glass in the bishops hosted in the devils seat forty one degrees and thirteen minutes north east and by north main branch seventh limb east side shoot from the left eye of the deaths head a bee line from the tree through the shot fifty feet out

9.5 Edgar Poe et la cryptographie

La vie d'Edgar Poe est pleine de drames. Il naît à Boston le 19 janvier 1809. Ses parents se sont mariés le 14 mars 1806, sa mère étant une jeune

veuve de 19 ans ; ils sont comédiens, sans succès. Edgar à un frère plus âgé, qui mourra en 1831, et une sœur plus jeune qui vivra jusqu'en 1874. Son père disparaît sans qu'on sache ce qui lui arrive ; sa mère meurt de tuberculose en décembre 1811.

Edgar Poe est recueilli par John Allan, un négociant de tabac aisé, et sa femme ; il s'appellera désormais Edgar Allan Poe. Il suit les Allan en Angleterre, revient à Richmond en Virginie. C'est un élève très brillant, excellent sportif.

Il entre à l'Université de Virginie en 1826. John Allan l'en retire pour ses dettes de jeu. Poe rompt avec lui, s'engage dans l'armée (il sera affecté au fort Multrie, dans l'île Sullivan du *Scarabée d'or*), puis entre à West Point dont il se fait exclure en 1831, revient chez une sœur de son père.

Dans les années 1830, Poe écrit beaucoup, mais ne connaît pas le succès. Il vit dans la misère, s'enivre. Il épouse le 16 mai 1836 la fille de sa tante, Virginia, qui n'a pas 14 ans. On le suit dans ses efforts pour connaître des succès littéraires, travaillant dans des revues où il vend ses nouvelles, cherchant à créer sa propre revue.

Au début des années 1840, il est toujours sujet à des crises d'éthylisme. Sa femme souffre de la tuberculose, lui est attiré par d'autres femmes. En 1843, paraissent *Le scarabée d'or* et *Double assassinat dans la rue Morgue*, en 1845 *La lettre volée* et *Le corbeau*, un poème tragique immédiatement célèbre qui sera traduit par Baudelaire, puis Mallarmé. Il travaille toujours avec acharnement, s'enivre, est malade, constamment dans la misère, voit sa femme s'affaiblir ; elle meurt le 30 janvier 1847.

Durant les deux dernières années de sa vie, il est toujours ballotté entre son travail, sa santé, des recherches d'amours, l'alcool.

Poe construisait ses textes de façon extrêmement élaborée, mettant en place des raisonnements d'une rationalité apparemment parfaite. Il était fasciné par les énigmes et avait une sagacité exceptionnelle pour résoudre celle qui lui étaient posées, énigmes policières, énigmes de roman, énigmes cryptographiques. Il avait mis ses lecteurs au défi de lui adresser des textes chiffrés qu'il ne puisse pas déchiffrer (textes chiffrés avec des bijections, si j'ai bien compris ; l'un des textes reçus ne respectait pas cette règle et a été déchiffré récemment).

Il fait dire à Legrand son opinion sur la cryptographie :

Les circonstances et une certaine inclination d'esprit m'ont amené à prendre intérêt à ces sortes d'énigmes et il est vraiment douteux que l'ingéniosité humaine puisse créer une énigme de ce genre dont l'ingéniosité humaine ne

vienne à bout par une application suffisante. (Circumstances, and a certain bias of mind, have led me to take interest in such riddles, and it may well be doubted whether human ingenuity can construct an enigma of the kind which human ingenuity may not, by proper application, resolve.)

Jusqu'en 1977, il allait avoir raison.

9.6 La bijection drôle de la BD

Le génie de Franquin est étonnant. En deux images, il nous fait comprendre mieux qu'un enseignant de mathématiques peut-être, ce qu'est exactement une bijection.

Notons $\mathcal{A}$ l'ensemble des 26 lettres de l'alphabet français. La machine à écrire remontée par Gaston tape les 26 lettres de l'alphabet, mais en désordre. Il s'agit donc bien d'une bijection, décrite en partie puisque qu'elle contient un cycle : $(A\ O\ I\ U\ L\ P\ Q\ R\ X\ldots)$ (lire A donne O qui donne I qui donne $U\ldots$ la dernière lettre du cycle donnant A) ; on ne sait s'il y a des points fixes (des lettres qui restent toujours tapées par la bonne touche) ni si elle est composée d'un ou plusieurs cycles. Gaston donne même un aperçu de la bijection inverse : $(L\ U\ I\ O\ A\ldots)$.

9.7 Chiffrements par bijection

Le principe du chiffrement par bijection est donc très simple. On se donne un ensemble $\mathcal{E}$ de 26 signes, chacun chiffrant une lettre de l'alphabet $\mathcal{A}$, ce qui revient à se donner une bijection $c : \mathcal{A} \to \mathcal{E}$. Les signes de $\mathcal{E}$ peuvent avoir des tracés compliqués ou bizarres, cela ne crée aucune difficulté supplémentaire

pour la cryptanalyse, contrairement à ce qu'on a pu penser). Par exemple, lSi on veut chiffrer un texte avec des chiffres ou des signes de ponctuation, il suffit de choisir un ensemble $\mathcal{E}$ un peu plus gros. On supprime en général les blancs, car laisser apparent le découpage en mots du message donne beaucoup d'informations à l'ennemi.

Le chiffrage du texte consiste à remplacer chaque lettre du message qu'on veut transmettre par son image par c.

Dans *Le scarabée d'or*, on ne connaît que 20 éléments de $\mathcal{E}$ et on remarque que $\mathcal{E}$ et $\mathcal{A}$ ont une intersection non vide. Pour la machine à écrire de Gaston, on peut supposer $\mathcal{E} = \mathcal{A}$.

La méthode de déchiffrement décrite par Edgar Poe dans *Le scarabée d'or* est connue depuis longtemps. Dans un texte retrouvé en 1987, al Kindi (vers 805-873) expliquait déjà qu'il fallait repérer dans un texte de la langue du message à déchiffrer quelle était la lettre la plus fréquente, la seconde lettre la plus fréquente, etc., puis repérer dans le message à déchiffrer le signe le plus fréquent, le second signe le plus fréquent, etc. et associer les uns aux autres. Cet exposé est trop systématique et ne convient pas dans la pratique ; on a vu que Legrand n'applique cette méthode qu'au signe le plus fréquent et que d'autres considérations interviennent pour la suite de son déchiffrement. La méthode d'al Kindi est reprise dans un traité d'al Qalqashandi (vers 1355-1418) de 1412.

9.8 Le chiffrement de Jules César

Les fouilles menées près d'Arles dans le Rhône ont livré ces derniers temps des statues magnifiques. Le fait que Jules César (de juillet -100 environ au 15 mars -44) chiffrait ses messages est rapporté par Suétone dans *La vie des douze Césars* (vers 120, sous Hadrien) à la fin du livre sur Jules César :

On a conservé en outre ses lettres à Cicéron et celles qu'il adressait à ses familiers sur ses affaires domestiques. Quand il avait à leur faire quelque communication secrète, il usait d'un chiffre, c'est-à-dire qu'il brouillait les lettres de telle façon qu'on ne put reconstituer aucun mot. Si on veut en découvrir le sens et les déchiffrer, il faut substituer à chaque lettre la troisième qui la suit dans l'alphabet, c'est-à-dire le D à l'A et ainsi de suite.

Cette traduction m'a été certifiée correcte par un latiniste de mes amis alors que la traduction habituelle dit que le procédé de Jules César est exactement l'inverse : il *consistait à changer le rang des lettres dans l'alphabet,*

en écrivant la quatrième pour la première, c'est-à-dire le D pour l'A, et ainsi de suite.

Je ferai deux remarques sur cette seconde traduction ; la première est une remarque de détail : le texte latin dit bien *quartam*, mais notre usage est de dire que le D est la troisième lettre de l'alphabet après l'A, et non la quatrième. La seconde est que je ne suis pas latiniste pour trancher, alors je donne le texte latin :

Extant et ad Ciceronem, item ad familiares domesticis de rebus, in quibus, si qua occultius perferenda erant, per notas scripsit, id est sic structo litterarum ordine, ut nullum uerbum effici posset : quae si qui inuestigare et persequi uelit, quartam elementorum litteram, id est D pro A et perinde reliquas commutet.

Examinons le procédé de Jules César en admettant que la bonne traduction est que le chiffrage consiste à remplacer chaque lettre par la troisième qui la suit dans l'ordre alphabétique comme tout le monde le dit.

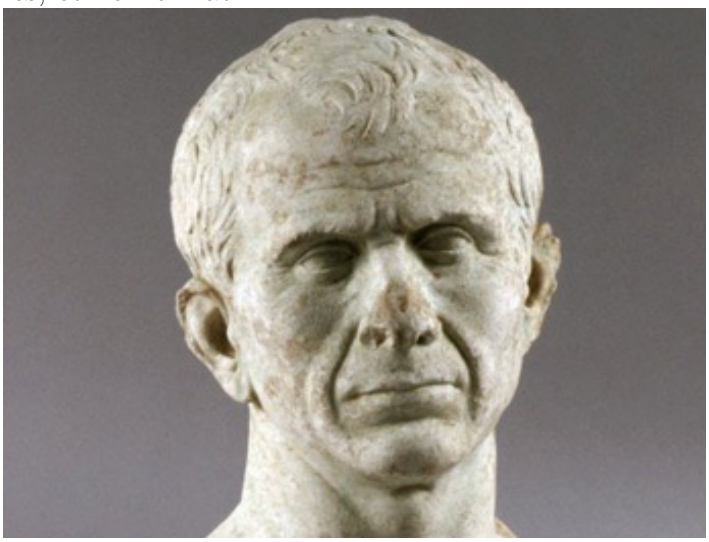
Chiffrage :

$LADOUCEURANGEVINE \rightarrow ODGRXFHXUDQJHYLQH$

Déchiffrage :

$DOHDMDFWDHVW \rightarrow ALEAJACTAEST$

Ajoutons que les célèbres paroles (*Iacta esto alea* écrit Suétone) prêtées à Jules César quand il franchit le Rubicon le 11 janvier -49, pour affronter le Sénat romain, auraient été dites (si elles le furent) en grec, la langue des élites romaines, et non en latin.



Pour les lettres de la fin de l'alphabet, on compte cycliquement : A, B, C chiffrent respectivement X, Y, Z. Notons aussi qu'à l'époque de Jules César, l'alphabet n'avait pas que 20 lettres ($I = J$, $U = V$, G, Y, Z ne font pas partie de l'alphabet romain archaïque), W n'existe pas).

On peut généraliser l'idée de Jules César en décalant les lettres de l'alphabet de façon cyclique et en définissant le décalage J_x par l'image x de la lettre A. On définit ainsi 26 décalages différents. Par exemple, J_R est le décalage : $A \to R$, $B \to S$, ..., $Y \to P$, $Z \to Q$.

Ces décalages peuvent être décrits très simplement en utilisant l'arithmétique modulaire, ce qui va nous permettre en même temps de donner une idée de ce qu'est un *changement de base*.

Il est naturel d'associer à chaque lettre de l'alphabet son rang, 1 pour A, 2 pour B, ... Autrement, dit, en posant $\mathcal{E} = \{1, 2, \ldots, 26\}$, on utilise la bijection de *nu*mérotation :

$$\nu : \mathcal{A} \to \mathcal{E}$$

et $\mathcal{E}$ s'identifie à l'ensemble des éléments de l'anneau $\mathbb{Z}/26\mathbb{Z}$. Le chiffrage J_x de Jules César, où x désigne la r-ième lettre après A (c'est-à-dire la lettre de rang $r+1$), correspond à l'application $\tau_r : k \mapsto k + r$. On peut exprimer le chiffrage J_x comme le composé : $\nu^{-1} \circ \tau_r \circ \nu$; autrement dit, pour trouver l'image d'une lettre par J_x, on regarde le rang de la lettre (on prend son image par ν), on décale le rang de r par τ_r et on regarde la lettre ayant le rang obtenu. Tout cela est contenu dans le diagramme commutatif qui visualise bien cette composition quand on en a l'habitude :

$$\begin{array}{ccc} \mathcal{A} & \xrightarrow{\varphi} & \mathcal{A} \\ {\scriptstyle\nu}\downarrow & & \uparrow{\scriptstyle\nu^{-1}} \\ \mathcal{E} & \xrightarrow[\tau_r]{} & \mathcal{E} \end{array}$$

La méthode de chiffrage de Jules César correspond à l'application : $x \mapsto x + 3 \mod 26$ et le déchiffrage est décrit par $x \to x - 3 \mod 26$. C'est la porte ouverte au rôle actuel de l'arithmétique dans les méthodes cryptographiques. Mais l'interprétation de ce chiffrage à l'aide de l'arithmétique modulaire remonte à un article de 1888 de Gaëtan de Viaris (1847-1901). On peut être surpris de cette date : elle paraît récente ; mais il faut penser que l'arithmétique modulaire est inventée par Gauss vers 1800 et que les spécialistes de cryptographie sont rarement des mathématiciens à cette époque.

Les systèmes UNIX utilisent aujourd'hui le chiffrage de Jules César avec décalage de 13 lettres : il suffit de l'appliquer une seconde fois pour retrouver le message initial ; ce n'est évidemment pas pour assurer la sécurité, juste, par exemple, pour éviter de dévoiler la solution d'un casse-tête.

9.9 Cage à Porcs

La méthode de la cage aux porcs ne pose aucun problème sérieux. Elle est très populaire depuis la Renaissance (on la trouve par exemple dans la *Polygraphiæ* de Trithème sous le nom d'*Enn'agrammaton*), mais ce n'est qu'un chiffrement par bijection (il y a des variantes). Des prisonniers l'utilisaient durant la guerre de Sécession ; un collègue m'a confirmé qu'il est connu des lycéens de nos jours. On part du dessin suivant.

A B C	D E F	G H I
J K L	M N O	P Q R
S T U	V W X	Y Z

Figure 2

Chaque lettre est chiffrée avec le contour de la case à laquelle elle appartient et un petit cercle ou un point indiquant sa position dans la case. Par exemple, DU serait chiffré :

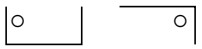


Figure 3

9.10 Gabriel de Lavinde

Le développement de la cryptographie est lié aux échanges diplomatiques. À la Renaissance, ce sont d'abord les cryptologues du pape, du gouvernement de Venise ou d'autres grandes cours italiennes qui y contribuent.

C'était du temps (1309-1418) où les papes étaient installés en Avignon, sous la surveillance du roi de France qui avait ses forteresses de l'autre côté du Rhône, à Villeneuve lès Avignon. Le grand schisme commence 1378. En Avignon, le secrétaire du pape (ou plutôt antipape) Clément VII s'appelle Gabriel de Lavinde ; on conserve au Vatican ses indications cryptographiques. Il donne un alphabet de chiffrement et surtout, cela semble une idée nouvelle, des chiffrages d'une douzaine de noms propres et de noms communs (12 selon Kahn, 24 selon l'Encyclopedia Britannica ; je n'ai trouvé aucun renseignement précis sur ce texte). La cryptographie n'était pas une nouveauté à l'époque ; l'idée de *répertoire* (on dit aussi *nomenclature*) est-elle vraiment née avec Gabriel de Lavinde ? Je ne sais ; en tout cas, elle allait être l'un des principaux outils des cryptographes pendant 500 ans.

9.11 Améliorations vaines

Au cours des quinzièmes et seizièmes siècles, les chiffreurs crurent apporter des améliorations au chiffrage par bijection. On imagina en 1401 à Mantoue de chiffrer les voyelles *a, e, i, o, u* par quatre ou cinq signes pour éviter que sa grande fréquence apparaisse (voir [Schneier] p. 11 ou Kahn p. 20). L'idée de chiffrages multiples d'une lettre fut étendu aux consonnes au XVI$^{\text{Øme}}$ siècle. Peine perdue ; les déchiffreurs tinrent compte d'autres particularités, comme de remarquer qu'un signe est toujours suivi ou précédé du même signe, ce qui permet de reconnaître le groupe *QU* en français. On imagina aussi d'introduire des signes indiquant que certains éléments du message devaient être considérés comme nuls. Cela ne créait pas de grande difficulté au déchiffreur. Il fallait de nouvelles idées.

9.12 Leon Battista Alberti (1404-1472)

Alberti est un humaniste remarquable du quinzième siècle. Il disait des mathématiques : *Rien ne m'aide plus à chasser la tristesse*, ce qui le rend tout de suite sympathique. Sa participation à l'invention de la *camera oscura* (une

boîte percée d'un trou sur le fond de laquelle on voit l'image inversée du paysage), vers 1432-34, n'est pas assurée. On a vu qu'il écrit le texte fondateur de la représentation en perspective centrale. Alberti s'impose comme architecte et ses travaux sont nombreux ; il publie en 1452 le *De Re ædificatoria* ; il a aussi l'idée de triangulation pour connaître une longueur non mesurable directement sur un terrain et est connu pour de nombreuses œuvres littéraires publiées tout au long de sa vie.

Vers 1460, le secrétaire pontifical parle des problèmes de cryptographie à Alberti. Le travail d'Alberti sur la cryptographie : *De componendis cyphris*, est présenté dans un texte en latin de 25 pages, écrit en 1466 ou 1467. Alberti analyse d'abord les défauts des chiffrages en usage à son époque, puis présente son système qu'il proclame, c'est une habitude chez les cryptographes, absolument incassable.

Pour pallier les défauts des chiffrages avec une bijection de l'alphabet, Alberti a l'idée de choisir plusieurs chiffrages différents et de changer de chiffrage d'un groupe de lettres à un autre, ce qui fait qu'une même lettre peut être codée de plusieurs manières différentes et que les calculs de fréquence ne donnent plus la possibilité du déchiffrement.

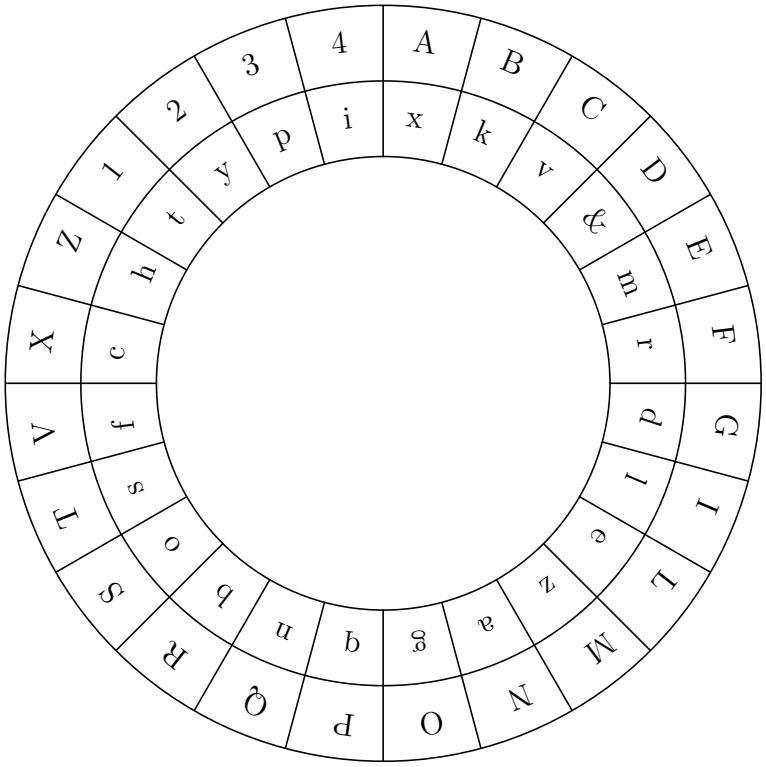
Pour réaliser cette idée et faciliter le travail, Alberti invente un système constitué d'un disque central qu'on peut faire tourner dans une couronne fixe (on parle de *disque chiffrant*. Les deux sont divisés en 24 secteurs égaux. Sur les secteurs de la couronne extérieure, on écrit les lettres de l'alphabet, sans J, U, W qui ne sont pas encore utilisés, ni H, K, Y ce qui permet, en ajoutant les chiffres 1, 2, 3 et 4 d'obtenir 24 signes. Sur les secteurs du disque intérieur, on écrit les 23 lettres de l'alphabet (y compris h, k, y) dans le désordre et un dernier secteur portant, dans certaines versions, le signe &. Chacune des 24 positions possibles du disque par rapport à la couronne donne un codage des lettres extérieures par les lettres intérieures et le &.

Pour savoir comment placer le disque et la couronne au départ, les correspondants conviennent d'une lettre du disque central, disons x, jouant le rôle de clé secrète. La première lettre du message codé indique la lettre de la couronne à mettre en face du x. Chaque changement de position est indiqué en écrivant la lettre à mettre en face du x.

Alberti conseille de changer la position du disque tous les trois ou quatre mots. C'est une idée absolument nouvelle, semble-t-il, et qui sera reprise sous des formes diverses pendant les siècles suivants (jusqu'à ENIGMA).

La seconde idée d'Alberti est d'avoir une nomenclature de certains mots ou phrases, codée par des groupes de deux, trois ou quatre chiffres de l'en-

semble $\{1, 2, 3, 4\}$, ce qui donne $4^4 + 4 \times 3^3 + 6 \times 2^2 = 382$ possibilités. Ces groupes de chiffres seront ensuite codés avec le disque, ce qui donne un surchiffrage, idée tellement novatrice qu'elle ne sera reprise que 400 ans plus tard.



Disque d'Alberti.

Le déchiffrage de messages chiffrés avec le disque d'Alberti n'est pas difficile si on connaît le disque utilisé : puisqu'Alberti chiffre deux ou trois mots sans changer son disque de position, la clé utilisée se trouve en essayant différentes positions jusqu'à ce que les premiers mots deviennent intelligibles.

De tels disques chiffrants étaient encore utilisés par les Confédérés pendant la guerre de Sécession.

9.13 Quelques noms autour de 1500-1550

David Kahn (voir pages 23-24) cite Giovanni Soro (mort en 1544) comme le grand cryptanaliste du début du seizième siècle. Il est service de Venise depuis 1506 pour cela, déchiffrant des messages des empereurs Maximilien I^{er} et Charles Quint. Sa renommée était telle que le pape lui demandait de déchiffrer les messages que ses services ne parvenaient pas à lire. Son traité de cryptologie est perdu.

Vigénère évoque les qualités de Philibert Babou (monsieur de la Bourdaisière), le cryptanaliste de François 1er : *Nonobstant tout cela l'industrieuse et vive conjecture des hommes ne laisse d'en venir à bout et pénétrer dans le secret, bien qu'avec un travail extrême d'esprit et un rompement inestimable de tête. Car je me resouviens d'avoir vu en mes jeunes années, étant nourri avec le général Bayard, premier secrétaire d'état du grand Roy François, feu monsieur de la Bourdaisière, aïeul de ceux qui vivent pour le jourd'hui, avoir souvente-fois déchiffré, sans l'alphabet faut-il entendre, plusieurs dépêches interceptées, en espagnol, en italien, allemand, ores qu'il n'y entendit rien, ou bien peu, avec une patience de trois semaines à y travailler continuellement jour et nuit, premier qu'en pouvoir tirer un seul mot : cette première brêche faite aussi, tout le reste vient bientôt après, tout ainsi qu'un démolissement de murailles.* Nous avions déjà noté dans la démarche de Legrand que la première victoire sur un texte chiffré entraîne toutes les autres. On dit aussi que toutes ces nuits passées à déchiffrer le courrier du roi n'étaient pas perdues pour tout le monde : si Philibert Babou les passait à déchiffrer ses dépêches, François 1er en profitait pour défricher son épouse, Marie Gaudin, avec laquelle il entretint une longue liaison.

9.14 La table de l'abbé Trithème (1462-1516)

Johann Heidenberg est né à Trittenheim, près de Luxembourg, sur les bords de la Moselle ; son nom latin a été francisé en Jean Trithème. À 21 ans, il est abbé près de chez lui, à Sponheim, puis un peu plus loin (200 kilomètres plus à l'est), entre Mayence et Nüremberg, à Würzburg, en 1506. C'est un grand érudit et collectionneur de livres. Il écrit les tout premiers traités de cryptographie.

La *Steganographia* (une lettre indique qu'il y travaille en 1499 et des copies manuscrites circulent peu après) parle de messages secrets envoyés

par les anges : il s'agit en réalité de cryptographie, mais la réputation de Trithème comme occultiste est établie et cela aurait pu être très dangereux pour lui : le livre, publié en 1506 et 1508, est mis à l'index en 1609. Le livre III de l'édition de 1508 contient des messages chiffrés simplement et sans intérêt, mais qui n'ont été déchiffrés que récemment (indépendamment par Thomas Ernst, 1996, et Jim Reeds, 1998).

La : *Polygraphiæ libri sex...* est publiée en 1518, mais la dédicace est de 1508. Il est réimprimé à plusieurs reprises, traduit en français en 1561. Certains y voient beaucoup de langage alchimique et une série de belles gravures est hermétique. Trithème a des idées un peu bizarres, comme de chiffrer les lettres de l'alphabet par des mots pieux : *a=Deus ou clemens, b=Creator ou clementissimus, etc.* (il donne une série d'équivalents pour chaque lettre) ; le chiffrage d'un mot a, quand les équivalents sont bien choisis (cela ressemble un peu aux *Cent mille milliards de poèmes* de Raymond Queneau), l'aspect d'une prière innocente ; le système est évidemment très peu sûr. Un exemple en français, maintes fois cité sur le web :

Dans la félicité (R) à perpétuité (E),
Dans son royaume (T) à perpétuité (E),
En Paradis (N) à perpétuité (E),
Ainsi qu'en toute éternité (Z) ;
Dans la gloire (L) à perpétuité (E),
Mais dans son règne (S) ;
Sempiternel (F), toujours (O) dans la félicité (R),
Tant dans la lumière (M) que dans la béatitude (U),
Et dans la gloire (L) à perpétuité (E),
Mais dans son règne (S) ;
En une infinité (D) encore à perpétuité (E),
Comme dans la gloire (L) autant que dans les Cieux (A),
A tout jamais (B), oui ! à tout jamais (B) à perpétuité (E) ;
Dans son royaume (T) et dans la félicité (R),
Irrévocablement (I), dans son royaume (T),
Et sans cesse (H) qu'il soit à perpétuité (E) dans la lumière (M),
Et encore à perpétuité (E) !

(RETENEZ LES FORMULES DE LABBE TRITHEME)

La grande innovation du livre est le tableau carré (*recta transpositionis tabula*) où les lettres sont présentées en colonnes la première dans l'ordre alphabétique de A à Z, la deuxième décalée d'un cran par rapport à la précédente : de B à Z, puis A, la troisième décalée d'un cran par rapport

à la deuxième : de C à Z, puis A, B.

Pour se servir de sa table, Trithème propose d'utiliser successivement les 24 colonnes et de recommencer. On chiffre la première lettre avec la première colonne, sans décalage, la seconde avec la seconde colonne, ce qui fait utiliser un décalage de Jules César d'une lettre, etc. Il donne également, semble-t-il, un exemple où les colonnes ne sont pas utilisées dans l'ordre.

9.15 Giovan Battista Bellaso (1505-vers1570/80)

Il est né à Brescia, étudie à Padoue ; sa famille est aisée. Il est au service d'un cardinal ; quand celui-ci est à Rome, Bellaso doit chiffrer les lettres qu'il lui envoie. La cryptographie intéresse alors les cours italiennes et on presse Bellaso de publier ses méthodes. Il le fait dans trois livres successifs :

La cifra del Sig. Giovan Battista Belaso, gentil'huomo bresciano, Venise, 1553 ;

Novi et singolari modi di cifrare, Brescia, 1555 ;

Il vero modo di scrivere in Cifra con facilità, prestezza, et securezza. Le traité de 1553 ne donne qu'un *l* à son nom ; c'est une erreur, mais c'est sous cette forme que so nom est en général cité.

C'est dans ce livre que Bellaso propose pour la première fois l'usage de clés. Il donne une table de 11 bijections de l'alphabet, à chacune desquelles il associe deux lettres de l'alphabet ; par exemple, la bijection associée à M et N échange a et r, b et s, c et t, etc. On notera que ces bijections sont simples : ce sont des involutions, c'est-à-dire qu'en appliquant deux fois la bijection, on obtient l'identité (voir la table plus loin).

Donnons l'exemple de Bellaso. Les deux correspondants conviennent d'une clé, un mot ou d'un bout de phrase comme VIRTUTI OMNIA PARENT qui va leur servir à chiffrer les messages qu'ils s'adressent quand ils sont éloignés. On colle les lettres et on les répète autant de fois que nécessaire au-dessus de la phrase à chiffrer, ici *L'armata Turchesca partira a cinque di Luglio*. La première lettre de la clé, V, demande d'utiliser la bijection définie par V et X, bijection qui envoie l sur s (et réciproquement) ; par conséquent on chiffre le l avec un s ; de même, la bijection définie par la seconde lettre de la clé, I, conduit à chiffrer a par y, etc. On obtient donc (sans tenir compte des signes de ponctuation et des espaces) :

clé	VIRTUTIOMNIAPARENTVIRTUTIOMNIAPARENTVI
texte clair	larmataturchescapartiraacinquediluglio
texte chiffré	sybouеyldanuofszlpiincupnshmlrnxoiznrd

Le disque d'Alberti permettait des changements de bijection à des intervalles variables, la méthode du mot clé rend ces changements réguliers.

Dans son premier livre, les bijections étaient construites simplement en décalant d'un cran à chaque fois la seconde partie de l'alphabet (nopqrstuxyz) par rapport à la première. Dans son second livre, Bellaso introduit une complication : l'ensemble de la table doit être construite à partir d'une phrase clé. Les lettres définissant les 11 alphabets sont données par une phrase clé. Par exemple, dans la phrase *Arma uirumque cano troie qui primus ab oris*, les lettres *armuiqecnotpbs* apparaissent successivement et on complète par celles qui manquent *dfghlxyz*, pour avoir les 11 alphabets correspondants à RA, MV, QI, CE, NO, TP, SB, DF, GH, LX, YZ. Les onze alphabets s'obtiennent en prenant d'abord les consonnes de la phrase clé : *rmqcntpsb* complétées par *dfghlxyz*, puis en intercalant les voyelles (qui apparaissent dans l'ordre *auieo*) aux rangs multiples de 4 : *rmqa cntu psbi dfge hlxo yz*. On obtient enfin les onze alphabets de la même façon que ci-dessus comme on le voit ci-dessous.

Les tables de Bellaso, 1553 (à gauche), 1555 (à droite).

On utilise alors une seconde phrase clé pour chiffrer le texte avec ces alphabets.

Dans son troisième livre, Bellaso reprend ses travaux précédents ; il propose un système ingénieux de texte autoclave, un texte où la clé de chiffrement est donnée par le texte. Il explique aussi pourquoi un ballot de plume et un de fer lachés en même temps arrivent en même temps à terre, mais son explication est chiffrée et personne ne l'a déchiffrée depuis ; la question était dans l'air bien avant Galilée. Il exprime enfin son amertume de voir qu'un livre publié en 1563 reprenne sa méthode sans le citer. Il s'agit du livre de Porta ; cela porta effectivement de l'ombre à Bellaso dont les idées ont été attribuées à Porta.

9.16 Giovanna Battista Della Porta (vers 1535-40, 1615)

Porta est un napolitain ; il semble avoir été très précoce dès son adolescence. Il était passionné d'optique et avait installé chez lui, à Murano (l'île des artisans du verre toute proche de Venise) un cabinet de curiosités que Peiresc, parmi bien d'autres, visita. Il a fait de nombreuses expériences sur les miroirs, construit une chambre noire et même conçu un projet de lunette astronomique bien avant les Hollandais et Galilée.

Porta nous intéresse ici pour son livre de cryptographie : *De Furtivis Literarum Notis, vulgo de ziferis, libri quinque*, publié à Naples en 1563 et 1602. La version de 1602, consultable sur le site de l'université de Tours, comporte cinq livres. Même si on peut lui reprocher de ne pas avoir cité Bellaso, son traité va beaucoup plus loin et l'un comme l'autre ont beaucoup apporté à la cryptographie.

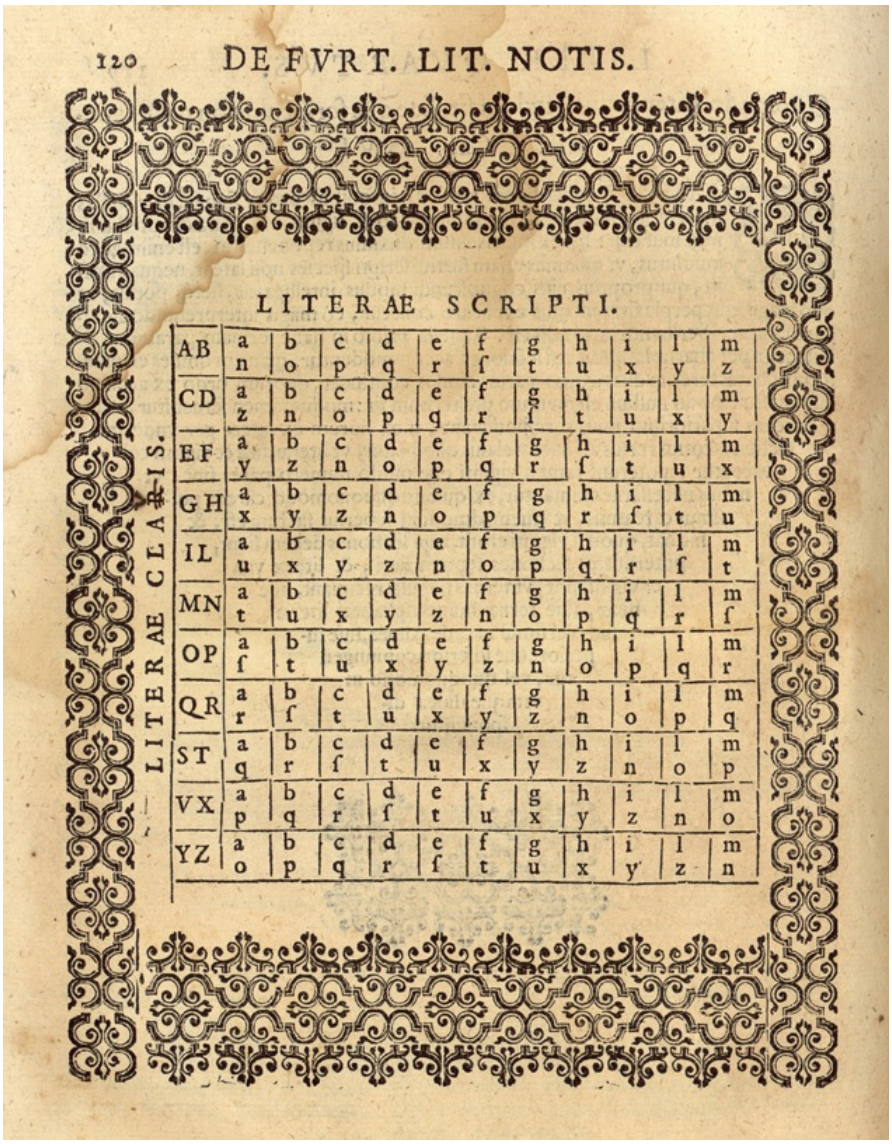
Le traité de Porta est peut-être le premier traité de cryptographie. Porta donne des aperçus historiques ; il s'efforce de classer les procédés, distinguant ce qu'on appelle les transpositions (où on ne fait que changer l'ordre des lettres du message) et les chiffrements par bijections avec des ensembles de lettres ou de signes.

Au livre III, il montre comment faire des transpositions : on écrit les lettres d'un texte dans une figure quadrillée, puis on écrit les lettres en suivant un parcours différent : par exemple, on écrit le texte horizontalement dans un rectangle de largeur fixée, puis on lit verticalement en remontant de bas en

haut et de gauche à droite les différentes colonnes ; ou encore en écrivant les lettres horizontalement dans un quadrillage ayant une forme triangulaire et en les lisant parallèlement à un des deux côtés obliques de ce triangle. Il est facile de reconnaître un texte soumis à une transposition : les fréquences des différentes lettres de la langue dans lequel il a été rédigé ne sont pas modifiées.

Pour les chiffrements avec des bijections variables (on parle de substitutions polyalphabétiques), Porta organise les idées de ses prédécesseurs.

Il reprend l'idée de Belaso du livre de 1553 :



120 DE FVRT. LIT. NOTIS.

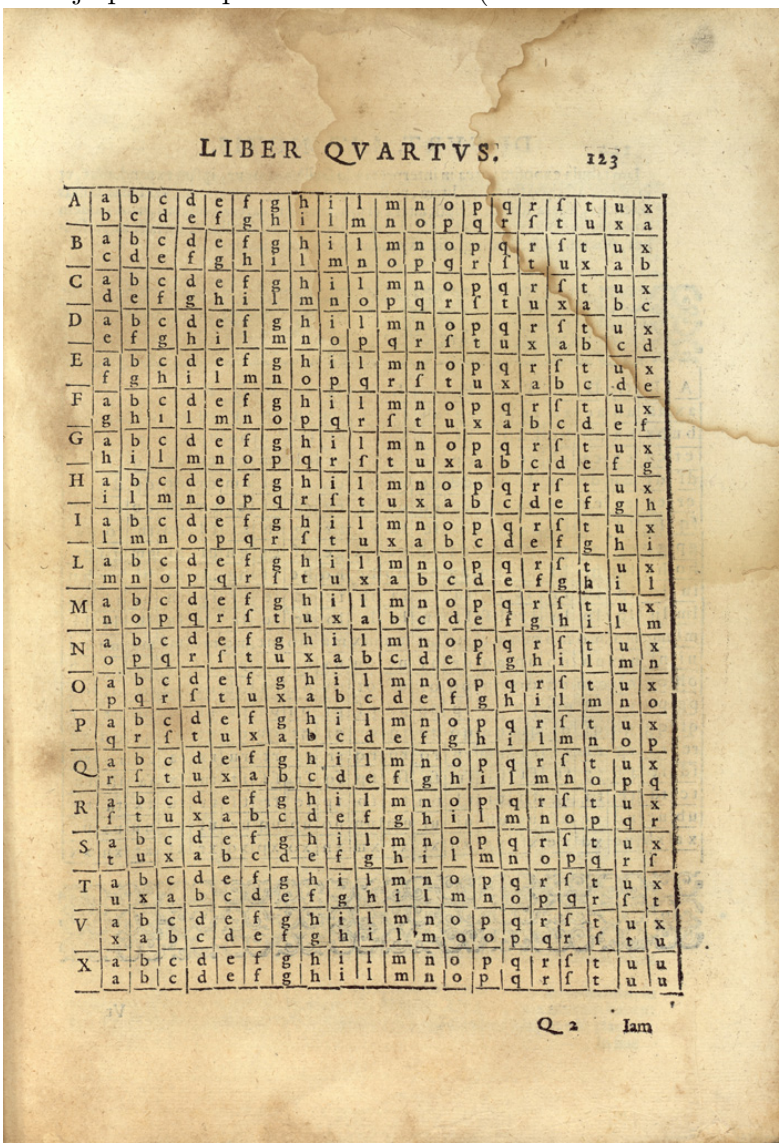
LITERAE SCRIPTI.

LITERAE CLAVIS.

AB	a n	b o	c p	d q	e r	f ſ	g t	h u	i x	l y	m z
CD	a z	b n	c o	d p	e q	f r	g ſ	h t	i u	l x	m y
EF	a y	b z	c n	d o	e p	f q	g r	h ſ	i t	l u	m x
GH	a x	b y	c z	d n	e o	f p	g q	h r	i ſ	l t	m u
IL	a u	b x	c y	d z	e n	f o	g p	h q	i r	l ſ	m t
MN	a t	b u	c x	d y	e z	f n	g o	h p	i q	l r	m ſ
OP	a ſ	b t	c u	d x	e y	f z	g n	h o	i p	l q	m r
QR	a r	b ſ	c t	d u	e x	f y	g z	h n	i o	l p	m q
ST	a q	b r	c ſ	d t	e u	f x	g y	h z	i n	l o	m p
VX	a p	b q	c r	d ſ	e t	f u	g x	h y	i z	l n	m o
YZ	a o	b p	c q	d r	e ſ	f t	g u	h x	i y	l z	m n

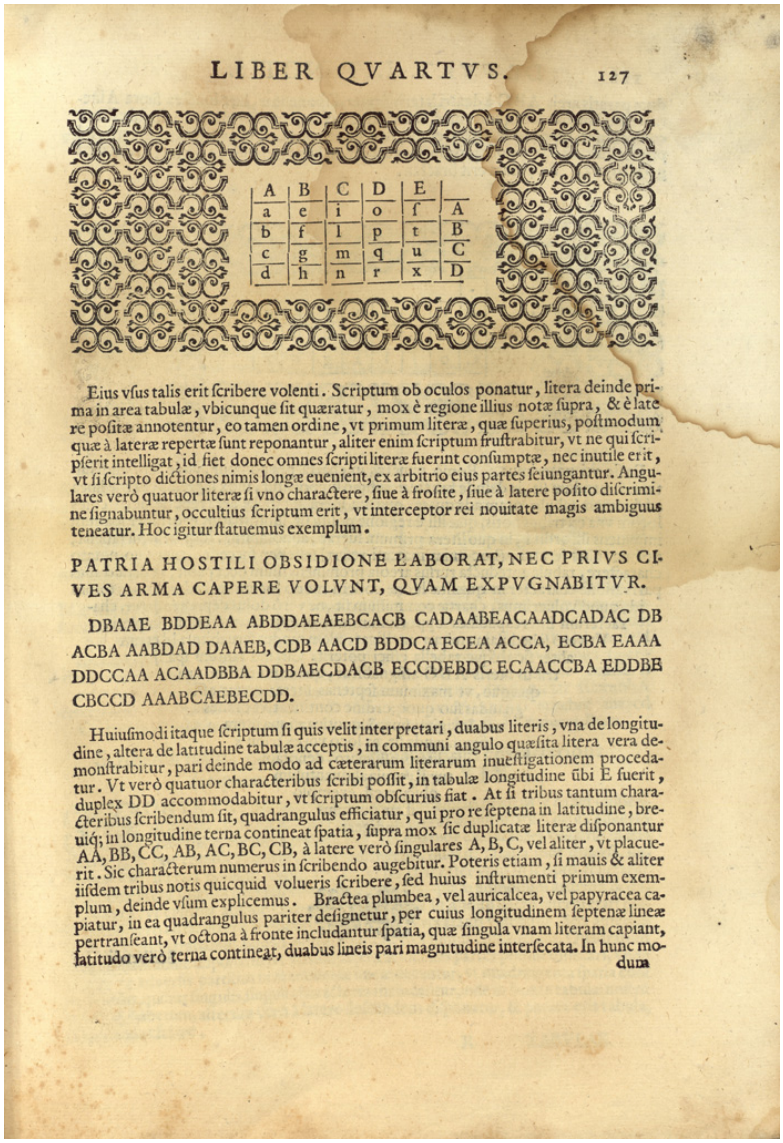
La table de Bellaso, Porta page 120.

Il donne ensuite des idées nouvelles, d'abord ce qu'on appelle carré de Vigénère dont je parlerai plus loin en détail (le X donne ici l'identité) :



Le carré de Vigénère Porta page 123.

Porta imagine aussi un rectangle de 5 sur 4 pour chiffrer les vingt lettres de l'alphabet :



LIBER QVARTVS. 127

A	B	C	D	E	
a	e	i	o	f	A
b	f	l	p	t	B
c	g	m	q	u	C
d	h	n	r	x	D

Eius vſus talis erit ſcribere volenti. Scriptum ob oculos ponatur, litera deinde prima in area tabulæ, vbicunque ſit quæratur, mox è regione illius notæ ſupra, & è latere poſitæ annotentur, eo tamen ordine, vt primum literæ, quæ ſuperius, poſtmodum quæ à lateræ repertæ ſunt reponantur, aliter enim ſcriptum fruſtrabitur, vt ne qui ſcripſerit intelligat, id fiet donec omnes ſcripti literæ fuerint conſumptæ, nec inutile erit, vt ſi ſcripto dictiones nimis longæ euenient, ex arbitrio eius partes ſeiungantur. Angulares verò quatuor literæ ſi vno charactere, ſiue à froſite, ſiue à latere poſito diſcriminе ſignabuntur, occultius ſcriptum erit, vt interceptor rei nouitate magis ambiguus teneatur. Hoc igitur ſtatuemus exemplum.

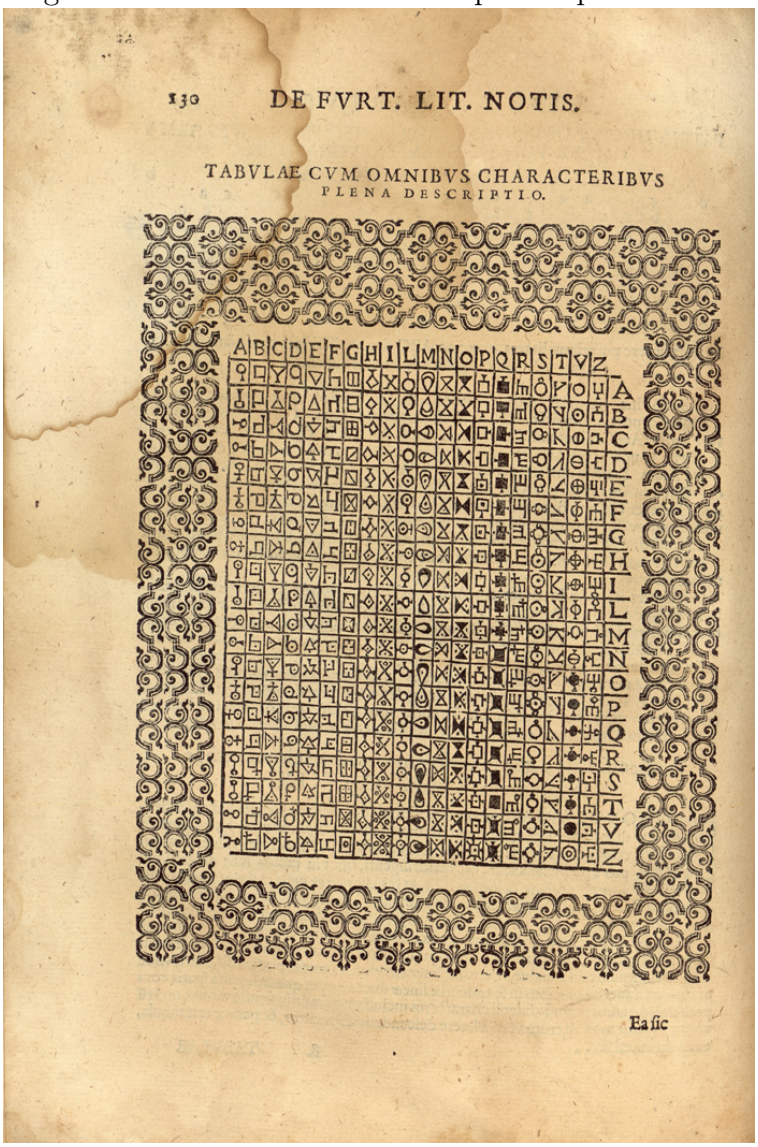
PATRIA HOSTILI OBSIDIONE LABORAT, NEC PRIVS CIVES ARMA CAPERE VOLVNT, QVAM EXPVGNABITVR.

DBAAE BDDEAA ABDDAEAEBCACB CADAABEACAADCADAC DB ACBA AABDAD DAAEB, CDB AACD BDDCA ECEA ACCA, ECBA EAAA DDCCAA ACAADBBA DDBAECDACB ECCDEBDC ECAACCBA EDDBE CBCCD AAABCAEBECDD.

Huiuſmodi itaque ſcriptum ſi quis velit interpretari, duabus literis, vna de longitudine, altera de latitudine tabulæ acceptis, in communi angulo quæſita litera vera demonſtrabitur, pari deinde modo ad cæterarum literarum inueſtigationem procedatur. Vt verò quatuor characteribus ſcribi poſſit, in tabulæ longitudine ſibi E fuerit, duplex DD accommodabitur, vt ſcriptum obſcurius fiat. At ſi tribus tantum characteribus ſcribendum ſit, quadrangulus efficiatur, qui pro re ſeptena in latitudine, breuiq; in longitudine terna contineat ſpatia, ſupra mox ſic duplicatæ literæ diſponantur AA, BB, CC, AB, AC, BC, CB, à latere verò ſingulares A, B, C, vel aliter, vt placuerit. Sic characterum numerus in ſcribendo augebitur. Poteris etiam, ſi mauis & aliter iiſdem tribus notis quicquid volueris ſcribere, ſed huius inſtrumenti primum exemplum, deinde vſum explicemus. Bractea plumbea, vel auricalcea, vel papyracea capiatur, in ea quadrangulus pariter deſignetur, per cuius longitudinem ſeptenæ lineæ pertranſeant, vt octona à fronte includantur ſpatia, quæ ſingula vnam literam capiant, latitudo verò terna contineat, duabus lineis pari magnitudine interſecata. In hunc modum

Le chiffrement de abcdefghilmnopqrstux par des couples, Porta page 127.

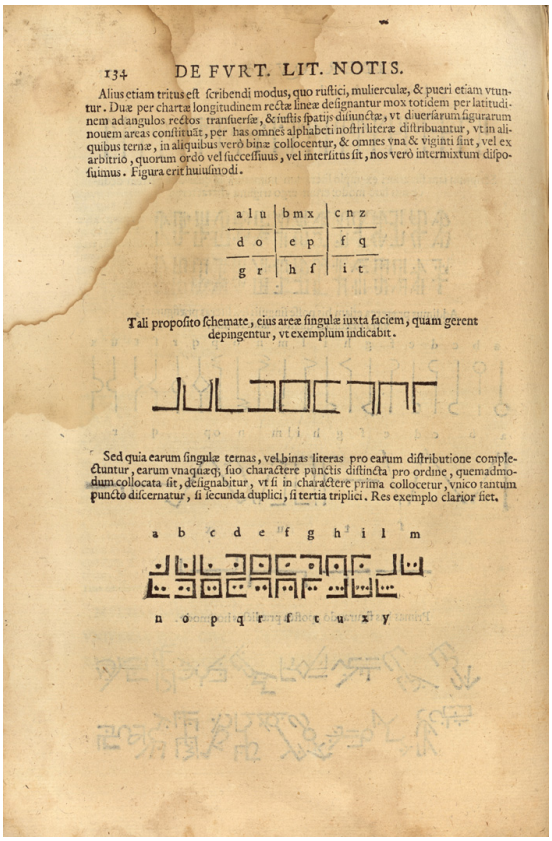
Porta imagine enfin de chiffrer les lettres par couples :



Le chiffrement des couples, Porta page 130.

Le livre comporte enfin des suggestions pour le déchiffrement, comme celle de rechercher un mot probable.

Au passage, Porta dit tout le mal qu'il pense du système de la cage aux cochons.



134 DE FVRT. LIT. NOTIS.

Alius etiam tritus eſt ſcribendi modus, quo ruſtici, mulierculæ, & pueri etiam vtuntur. Duæ per chartæ longitudinem rectæ lineæ deſignantur mox totidem per latitudinem ad angulos rectos tranſuerſæ, & iuſtis ſpatijs diſtinctæ, vt diuerſarum figurarum nouem areas conſtituãt, per has omnes alphabeti noſtri literæ diſtribuantur, vt in aliquibus ternæ, in aliquibus verò binæ collocentur, & omnes vna & viginti ſint, vel ex arbitrio, quorum ordo vel ſucceſſiuus, vel interſitus ſit, nos verò intermixtum diſpoſuimus. Figura erit huiuſmodi.

a l u	b m x	c n z
d o	e p	f q
g r	h ſ	i t

Tali propoſito ſchemate, eius areæ ſingulæ iuxta faciem, quam gerent depingentur, vt exemplum indicabit.

Sed quia earum ſingulæ ternas, vel binas literas pro earum diſtributione complectuntur, earum vnaquæq; ſuo characterе punctis diſtincta pro ordine, quemadmodum collocata ſit, deſignabitur, vt ſi in characterе prima collocetur, vnico tantum puncto diſcernatur, ſi ſecunda duplici, ſi tertia triplici. Res exemplo clarior fiet.

a b c d e f g h i l m

n o p q r ſ t u x y

La cage aux cochons, Porta page 134.

9.17 Blaise de Vigénère (1523-1596)

Vigénère est diplomate au service de la maison de Nevers. Il accompagne François de Clèves à Rome en 1549 ; il y entend parler des méthodes de Bellaso ; il y retourne en 1566. C'est là sans doute qu'il étudie la cryptographie de son temps ; il raconte y avoir vu déchiffrer des messages en turc. Il se retire des affaires en 1570, se marie, a des enfants. Il publie beaucoup : des œuvres anciennes comme le beau texte de Villehardouin sur la prise de Constantinople des années 1200, des traductions d'auteurs latins (César, Cicéron, Tacite), donne ses propres textes sur des sujets très divers, les comètes, etc. En 1584, il est secrétaire de Henri III.

Nous avons vu que l'idée d'Alberti de changer de code tous les deux ou trois mots avait été retravaillée au seizième siècle sous diverses formes.

Vigénère reprend les idées de Bellaso et Porta en présentant ce qui sera appelé plus tard carré de Vigénère dans son *Traité des chiffres ou secrètes manières d'écrire* (réédité en fac similé en 1996 par Guy Trédaniel) de 1586 ou il mêle la cryptographie a bien d'autres sujets : alchimie, idéogrammes japonais, kabbale, recettes pour fabriquer de l'or, etc.

Dans ce traité, il évoque (folios 34-35) les méthodes de son temps, les lettres chiffrées de plusieurs manières pour déjouer les analyses de fréquences et les nomenclatures : *Mais la plupart de ceux dont j'ai vu user ès cours des princes, consistent seulement en une multiplication de caractères faits à plaisir ; estimant que pour être bizarres, inconnus et en grand nombre, le sens qui y est contenu ne pourra être découvert sans la communication de l'alphabet ; car les voyelles, parce qu'elles sont plus fréquentes que les autres lettres y sont triplées et quadruplées, voire plus ; et le reste à l'équipollent ; avec des doubles des nulles et tout plein de notes à part qui désignent chacune un mot ; comme Empereur, Roy, armes, vivres, galères et autres semblables.*

La méthode du carré de Vigénère est ingénieuse, mais extrêmement simple en réalité. Vigénère prend une suite de lettres de longueur finie : $x_1 \dots x_n$. Il découpe son message en suites de longueur n (la dernière suite est de longueur inférieure ou égale à n). Si $a_1 \dots a_n$ est une telle suite, il la chiffre par $J_{x_1}(a_1) \dots J_{x_n}(a_n)$, autrement dit, il décale a_1 comme lui indique x_1, a_2 comme lui indique x_2, etc. Puis il recommence le même procédé pour les autres suites du message découpé.

Le premier problème pour des gens qui veulent communiquer avec ce code est de mémoriser la suite des x_i qu'on appelera la clé. Vigénère propose d'utiliser un mot ou une phrase qu'on peut mémoriser. Si ce mot est, par exemple, Juliette, on utilise successivement les décalages $J_j, J_u, J_l, J_i, J_e, J_t, J_t, J_e$, puis on recommence.

Ce codage revient à découper le texte en blocs m de longueur k égale à la longueur de la clé et à ajouter la clé, considérée comme un élément τ de $(\mathbb{Z}/26\mathbb{Z})^k$ à chaque bloc : la suite des $m' = m + \tau$ est le message transmis ; la suite $m' - \tau$ redonne le message initial.

Le second problème avec ce chiffrement est le risque d'erreur important : oublier un pas à un endroit rend la suite du texte inintelligible jusqu'à ce qu'on ait pu se recaler.

Vigénère souligne l'impossibilité de casser son système :

il est impossible par consequant, que coniecture aucune pour subtile qu'elle puisse estre ; ne patience & assiduité de labeur ; ne ruze & vsage des dechiffremens, peut iamais mordre sur cestuy-ci

Cependant, il envisage tout de même :

il est bien vray que tant plus longue est la clef, tant plus sera malaisé le chiffre à descouurir ; mais tant plus difficile aussi & embrouillé tant au chiffre qu'au dechiffrer...

Il n'aurait pas été désavoué par ceux dont nous allons parler plus loin.

La pratique montre que le système de Vigénère est assez lent à mettre en pratique, nécessitant beaucoup de soin ; il a longtemps été considéré comme très sûr. Nous verrons plus loin qu'il est possible de le casser, mais cela n'a été trouvé que près de 300 ans plus tard.

Simon Singh affirme péremptoirement : *En raison de sa force et de sa sécurité, on aurait pu croire que tous les secrétaires du chiffre en Europe adopteraient rapidement le chiffre de Vigénère. Or, ils l'ignorèrent avec un bel ensemble. Ce système apparemment sans défaut resta négligé pendant les deux siècles suivants.* Certes, les systèmes à nomenclature étaient considérés comme beaucoup plus commodes par beaucoup, mais je ne suis pas sûr que Singh ait vraiment raison : le texte de Vigénère a été traduit en italien en 1644 par Du Carlet, Dlandol cité plus loin en parle comme d'un système très utilisé ainsi que les auteurs des années 1880.

Une autre idée de Vigénère lui est vraiment propre ; il s'agit d'un système autoclave. Dans le choix de la clé, Vigénère dit qu'on peut choisir *le dernier mot qui precede l'escriture chiffree.* Il propose alors que la clé soit réduite à une seule lettre x *dont de main en main partira successiuement tout le reste, cõme si elles venoient à naistre les vnes des autres* et que la clé soit x suivie du texte du message ; si Roméo veut écrire à Juliette : *je t'aime à la folie* et qu'il a convenu avec elle de la clé *f*, il lui enverra *jetaimealafolie* chiffré avec la clé *fjetaimalafoli.* C'est une belle idée, mais il suffit de faire au maximum 26 essais pour déchiffrer le texte ; l'idée de Vigénère est stupide telle quelle, mais elle est intéressante si on utilise une clé un peu plus longue qu'une seule lettre. Ajoutons que cette nouvelle idée n'est pas sûre non plus. La technique est de supposer que le texte à chiffrer comporte nécessairement des mots simples comme LES en français ou THE en anglais. Puisque la clé est le texte en clair décalé, on regarde à différents endroits si le mot qu'on a choisi peut figurer dans le texte en clair ; si c'est le cas, la partie de la clé correspondante est une partie antérieure du message et se reconnaît pour être un mot ou une partie de phrase correcte ; le reste du déchiffrement sera aisé.

9.18 Les célèbres déchiffrements de François Viète

Le grand mathématicien de cette époque, François Viète (1540-1603), qui introduit, comme on sait, le calcul littéral en algèbre, s'est illustré en cryptographie. Pendant les derniers combats des guerres de religion, entre l'armée des catholiques de la Ligue et les forces de Henri III et du futur Henri IV, l'envoyé de Philippe II en France, Juan de Moreo, utilisait un code pour correspondre avec lui. Ce code, utilisait environ 400 signes (99 nombres pour les syllabes et 40 signes pour des lettres ou des mots suivant d'autres sources), mais François Viète, en travaillant d'arrache pied (du 28-10-1589 au 15-3-90) en vint à bout. Il publie alors *Deschiffrement d'une lettre escripte par le Commandeur Moreo au Roy d'Espagne son maître, du 28 octobre 1589*[2]. Cette lettre a donc été écrite trois mois après l'assassinat de Henri III par le moine Clément, le premier août et un mois après la victoire de Henri IV à Arques.

Jacques Auguste de Thou détaille cette réussite :

Et cette chose troubla beaucoup les Espagnols pendant deux ans, qui par le secret découvert au moyen de nos lettres interceptées à leur tour, étaient affligés par la nécessité de changer une méthode qu'ils pensaient inexplicable.

On raconte, en effet, que Philippe II, persuadé de l'inviolabilté de son système (c'est une erreur fréquente et dangereuse), alla jusqu'à accuser Viète de magie noire devant le pape. Mais le Vatican avait depuis longtemps son service spécialisé dans la cryptographie et ses spécialistes connaissaient, eux aussi (et sans l'aide du diable !), les codes de Philippe II. L'affaire ne fit que tourner un peu plus l'empereur espagnol en ridicule.

Le déchiffrement de Viète intervient juste après la victoire d'Ivry, qui donne à Henri IV un avantage décisif sur les forces de la Ligue. Habituellement, on ne divulgue pas le percement d'un code, pour pouvoir continuer à lire les lettres de l'ennemi. La publication de Viète a sans doute eu lieu pour des motifs politiques et à la demande de Henri IV. Elle montrait les ambitions du duc de Mayenne sur le trône de France, alors qu'en tant que

2. Il ne semble exister que deux exemplaires de cette lettre ; celui de la bibliothèque nationale serait annoté de la main de Viète ; Jean-Paul Guichard m'a permis d'en prendre connaissance ; Jean-Paul Guichard a aussi construit un site très riche sur Viète :http ://www.cc-parthenay.fr/parthenay/creparth/GUICHARDJp/VIETEaccueill.html.

lieutenant-général du royaume, il devait obéissance au Roi que la Ligue nommait, le 5 mars 1690, le cardinal Charles de Bourbon, un éphémère Charles X (mort le 5 mai suivant et rayé par la suite de la liste des rois de France). Il semble également que d'autres lettres de Philippe II furent transmises au duc de Mayenne pour lui montrer que le soutien de Philippe II n'était pas sans arrières pensées et le pousser à accepter un compromis avec Henri IV.

Je ne sais ce que Viète pensait du carré de Vigénère ; nous ne le connaissons que par ses talents de déchiffreur. Comment faisait-il ? Juste avant sa mort, il a laissé un texte où il donne quelques explications sur ses méthodes. Ce texte a été analysé récemment (Pesic, Cryptologia vol. XXI, n° 1, janvier 1997). Viète avait remarqué que sur trois lettres successives, une au moins était une voyelle ; une étude des suites de trois lettres le conduisait à les découvrir.

9.19 Voyage à Venise

Le Conseil s'occupait surtout du renouvellement de ces inventions pour dérouter le mieux possible la curiosité des cabinets étrangers et mettre en défaut l'habileté de ceux qui s'exerçaient à en découvrir le secret, dans l'intérêt des Ministres qu'ils servaient. Lorsque le Conseil des Dix avait conçu le moindre soupçon sur la pénétration de l'un de ses alphabets en chiffres, il en déclarait aussitôt la nullité et ordonnait une sorte de concours pour que l'alphabet fut promptement remplacé. Trois de ses membres étaient choisis pour juger de la meilleure et de la plus sûre invention. Ces juges devaient présenter chacun un rapport aux chefs du Conseil sur les qualités, les défauts ou les inconvénients des compositions que leur avaient présentées les secrétaires députés aux chiffres.

Ces procédures furent mises en œuvre quand l'Ambassadeur de Venise Giovanni Mocenigo eut une grande surprise au cours d'un entretien avec Viète. Laissons-le le raconter, dans une lettre du 5 juin 1595 : *Je me trouvais à Tours où, m'entretenant un jour avec M. de Viète, il en vint à me dire qu'on avait intercepté un très grand nombre de lettres en chiffres, tant du roi d'Espagne que de l'Empereur et autres princes, lesquelles avaient été déchiffrées et interprétées par lui... et comme je lui montrais beaucoup d'étonnement, il me dit : « J'en donnerai des preuves effectives à Votre Seigneurie ». Il m'apporta aussitôt un gros paquet de lettres desdits Princes qu'il avait déchiffrées et ajouta : « Je veux que vous sachiez que je comprends et que je traduis*

votre chiffre ». Je ne veux pas le croire, dis-je, à moins que je ne le voie. Et comme j'avais trois sortes de chiffres, un ordinaire dont j'usais, un autre différent dont je n'usais pas et le troisième appelé dalle caselle, il me montra qu'il comprenait le premier. Pour mieux pénétrer alors ce qu'il en était dans une affaire aussi grave, je lui dis : « Vous comprenez sans doute aussi notre chiffre dalle Caselle ? »Il répondit : « Pour celui-là, il faut en sauter beaucoup », voulant dire qu'il ne comprenait que par morceaux.

Je trouve extraordinaire d'entendre, presque comme un enregistrement très ancien, Viète parler. On s'aperçoit également qu'il n'était pas un cryptographe occasionnel. L'ambassadeur ajoute : *J'ai gardé tout cela bien en mémoire, étant chose d'une importance bien reconnue de Vos Seigneuries et j'ai voulu vous le faire savoir, afin que soient promptement prises les mesures qui paraîtraient nécessaires à la prudence de Vos Seigneuries.* Le 12 juin suivant, le Conseil des Dix changeait en effet tous ses chiffres pour des inventions nouvelles de Pietro Partenio, son chiffreur alors.

9.20 Les chiffres de Sully et Henri IV

On pourrait croire qu'en France, sous l'influence de Vigénère et Viète, le choix des systèmes de chiffrement ait évolué. Mais il n'en est rien. Quand Henri IV cherchant à lutter contre l'Autriche et l'Espagne, correspond avec le Landgrave de Hesse, entre 1602 et 1606, il chiffre les lettres avec des nombres de deux chiffres, quatre nombres pour a, e, i, n, o, r, s, u, z, trois ou deux nombres pour les autres lettres ; des syllabes, des mots sont chiffrés avec des signes spéciaux, des nombres éventuellement surmontés d'un tréma ou d'une barre : $\bar{45}$ est l'Électeur de Brandebourg, par exemple. Le système de Sully en 1599 est tout à fait analogue. Ces systèmes étaient utilisés sur de longues périodes, les ennemis devaient en venir à bout avec un peu de ténacité et la possibilité de les changer devait être un problème.

9.21 Le siècle des Rossignol

Lorsque le Prince de Condé assiège Réalmont, une petite ville du Tarn tenue par les Protestants, en 1629, une lettre chiffrée des habitants est interceptée. Le Prince fait appel à Antoine Rossignol (1600-1682), dont la réputation de déchiffreur était établie dans la région. Rossignol déchiffre fa-

cilement le message : les habitants rendaient compte de leur détresse ; quand le Prince leur communique leur message déchiffré, ils se rendent.

La réputation de Rossignol est établie et Richelieu le sollicite l'année suivante pour déchiffrer les lettres des Rochelais assiégés, puis l'attacher à son service. Rossignol change les méthodes du chiffrement par nomenclature en introduisant deux tables ; jusqu'à lui, une suite croissante de nombres correspondait à la suite des mots à chiffrer pris dans l'ordre alphabétique. La première table de Rossignol donne les mots (quelques centaines), classés par ordre alphabétique, avec les nombres (ou les groupes de lettres, cela dépend du chiffrage) qui leur sont associés. La seconde table donne les chiffres (ou les groupes de lettres) en ordre croissant, avec leurs significations. L'usage de ces tables, de plus en plus étendues, se conservera plus de 200 ans. Antoine Rossignol passe ensuite au service de Mazarin, puis de Louis XIV. Son rôle est important pendant 50 ans ; la protection du roi lui assure la richesse, il est anobli comme seigneur de Juvisy et recevra le roi de France dans son château. Son fils Bonaventure continue son travail.

Certains auteurs écrivent qu'on rendit hommage à l'ingéniosité des Rossignol en utilisant le terme de rossignol pour les crochets permettant de forcer les serrures, mais le Robert donne 1406 comme première apparition du mot dans ce sens, avec une origine obscure.

Aux XVII$^{\text{Øme}}$ et XVIII$^{\text{Øme}}$ siècle, chaque cour d'Europe a son cabinet noir cherchant à déchiffrer les lettres interceptées par ses agents. Une lettre de 1677 de Louvois montrant que le ministre de Louis XIV se souciait des problèmes de cryptographie : il demande qu'un nouveau chiffre soit toujours prévu en remplacement d'un chiffre qui ne pourrait plus être utilisé ; c'est très avisé.

9.22 Le masque de fer

Une autre lettre de Louvois, du 8 juillet 1691, aurait dû cesser de faire couler beaucoup d'encre une fois déchiffrée. Elle fait partie d'une série de sept lettres adressées au commandant en chef de l'armée du Piémont, Nicolas de Catinat (1637-1712) par Louvois et Louis XIV. Ces lettres n'ont pas été enregistrées aux Archives. Elles apparaissent en 1819, publiées par un descendant de Catinat ; elles sont chiffrées. En 1891, elles sont proposées à la sagacité du commandant Bazeries. Celui-ci parvient à un déchiffrement qu'il publie en 1893, en restituant le *Grand chiffre de Louis XIV*, chiffre dû

probablement à Bonaventure Rossignol. La découverte est sensationnelle : il s'agit de l'identité de l'homme dit *au masque de fer*, le fameux prisonnier de la forteresse de Pignerol (en Piémont, entre Briançon et Turin, *Pinerolo* en italien), emprisonné pendant 30 ans et qui devait mourir à la Bastille le 19 novembre 1703. On avait beaucoup écrit sur ce prisonnier depuis Voltaire et Alexandre Dumas (*Le Vicomte de Bragelonne*).

Le chiffre utilisait 587 nombres apparaissant chacun un certain nombre de fois dans les pages codées. Les premières attaques de Bazeries furent vaines : le chiffre n'était pas un chiffre codant les paires de lettres (il y a a priori 26 fois 26 = 676 paires différentes, ce qui est du même ordre que 587). Après des mois de travail, Bazeries eut une autre idée. Les nombres pouvaient coder des syllabes. L'ensemble des textes comportait 11125 nombres ; le nombre 22 apparaissait 187 fois, le nombre 124 apparaissait 185 fois, etc. La méthode de Bazeries était de supposer qu'un mot avait été utilisé et à rechercher son chiffrement. Puisqu'il s'agissait d'opérations militaires, il pensa au mot ENNEMI. Les groupes de nombres suivant pouvaient y correspondre.

124	22	146	46	469
124	22	125	46	574
124	22	125	46	120
124	22	125	46	584
124	22	125	46	345
124	22	125	46	345

L'hypothèse que le chiffrage soit celui de LES-EN-NE-MI-S conduisit au déchiffrement de 1077 entiers du texte. Bazeries repéra alors la suite 124.22.88.374.46 et y reconnu l'épellation de la syllabe NE en N-E ; il obtint alors la signification de 258 nouveaux entiers. Les déchiffrages déjà trouvés permirent d'avancer : ET-J'AI-53-É-QUE donna 53=ORDONN, L'-358-POUR- donna 358=ARGENT. Certains nombres ne codaient pas des syllabes mais des lettres , un nombre indiquait qu'il fallait effacer le nombre qui le précédait, etc.

La lettre de Louvois résultait d'un événement récent, une campagne des troupes de Louis XIV au Piémont, compromise par la lâcheté du général Vivien Labbé de Bulonde qui, chargé du siège de Cuneo, s'enfuit devant les troupes autrichiennes en laissant beaucoup de soldats blessés et de matériel. Louvois indiquait : *Elle (Sa Majesté) désire que vous fassiez arrêter M. de Bulonde et le fassiez conduire à la citadelle de Pignerol où Sa Majesté veut qu'il soit gardé, enfermé pendant la nuit dans une chambre de ladite citadelle et le jour ayant la liberté de se promener sur les remparts avec un 330-309.*

Les nombres 330 et 339 n'apparaissaient nulle part ailleurs, mais aucun doute n'était permis : 330=MASQUE, 309=un point de fin de phrase. L'énigme du masque de fer était enfin résolue : il s'agissait du général de Bulonde !

Ce déchiffrement ne semble pas avoir désarmé les amateurs de mystères et les interrogations sur le masque de fer ont eu encore de beaux jours devant elles. Cette lettre pouvait après tout avoir été écrite dans l'intention qu'elle soit déchiffrée afin de créer une fausse piste et ce serait bien le frère jumeau de Louis XIV qui aurait été emprisonné à Pignerol. Une cinquantaine d'hypothèses différentes ont été proposées sur l'identité du mystérieux prisonnier.

David Kahn (voir pages 72-73) semble mieux renseigné que Singh (voir page 73). Il dit que la vraie traduction est que le prisionnier pourra se promener sur les remparts avec un 330-339. Il ajoute que masque n'est pas un terme militaire et n'apparaît pas dans les répertoires de l'époque, que Bulonde était un personnage de second plan qui n'aurait pas mérité tout cet honneur et que (c'est tout de même un argument très fort !) qu'en 1708, plus de cinq ans après sa mort supposée, Bulonde était toujours vivant ! Robert Lamoureux aurait bien ri.

9.23 La cryptographie à l'époque de Napoléon

On pourrait penser qu'un général féru de mathématiques saurait s'entourer d'un service de cryptographie d'un bon niveau. Il semble qu'il n'en ait rien été et la cryptograhie sous l'Empire était loin de valoir celle du roi soleil. Les exemples que donne Bazeries dans un de ses livres sont consternants.

Un extrait d'une dépêche adressée à Augereau, le 17 septembre 1813 : *l'Empereur ordonne que vous vous portiez le plus tôt possible 167, 138, 169, 106, 171, 15, 117... Son principal but sera de rester 107, 87, 176, 169, 53, 52, 167, 52, 35, 138, 6, 85, 82, 52, 106, 171, 15, 117.* La solution est :

167, 138, 169, 106, 171, 15, 117 = s, u, r, la, sa, a, le ;

107, 87, 176, 169, 53, 52, 167, 52, 35, 138, 6, 85, 82, 52, 106, 171, 15, 117= ma, i, t, r, e, de, s, de, bo, u, c, h, es, de, la, sa, a, le.

L'alternance du texte en clair et du texte chiffré, la fragilité du système, la possibilité que l'ennemi en ait connaissance sont autant de faiblesses. Mais ce n'est pas tout ; un duplicata de la dépêche contenait le même texte mais avec beaucoup plus de passages chiffrés avec exactement le même système ;

si l'ennemi s'empare des deux dépêches, une simple lecture en parallèle lui donne sans effort une grande partie du système de chiffrement.

En 1814, les services cryptographiques n'existent plus et c'est en clair que Berthier envoie des ordres de regroupement (qui, pour la plupart, n'arrivèrent pas dans des mains françaises).

9.24 Deux siècles d'utilisation

La méthode de Vigénère ne semble pas très utilisée au début, les cryptographes préférant comme on l'a déjà dit, des systèmes de nomenclature. Mais un certain Dlandol affirme en 1793 : *Ce chiffre a été nommé le chiffre par excellence, parce qu'il réunit le plus grand nombre d'avantages que l'on puisse désirer pour une correspondance secrète. Il les réuniroit tous sans aucune exception, s'il n'étoit pas d'une exécution un peu lente ; mais il rachète bien cet inconvénient par la sûreté incroyable dont il est. Cette sûreté est telle que l'univers entier ne le connoitroit, si on ne savoit pas le mot de clef convenu entre les correspondants, on pourroit montrer sa lettre à tout le monde, sans que personne pût la lire.* La dernière affirmation est trop optimiste, comme on va le voir.

L'amiral anglais Francis Beaufort (1774-1857), un homme remarquable, descendant d'une famille protestante ayant quitté la France au moment de la Saint-Barthélémy, inventeur de l'échelle de Beaufort pour les vents, cartographe passionné, infatigable et dont les cartes sont célèbres, améliore l'idée de Vigénère en composant le chiffrage de Vigénère avec une symétrie $x \to 27 - x \bmod 26$ qui est très simple à mettre en pratique sur un tableau. L'idée avait déjà été trouvée par Giovanni Sestri en 1710.

Charles Babbage (1791-1871) renonce à la fortune familiale, invente un compteur de vitesse, un pare-buffles sur les locomotives, la dendrochronologie, s'occupe de statistiques et de table de mortalités, du prix des timbres poste, proposant qu'ils soient indépendants de la distance : l'économie réalisée dans le calcul du prix est plus importante que les bénéfices qu'on pourrait retirer du calcul d'un prix juste. Constatant, en 1821, avec l'astronome John Herschell, que le calcul à la main des tables mathématiques utilisées pour la navigation, etc. comportait des milliers d'erreurs entraînant des catastrophes, naufrages, etc., il entreprend de dresser les plans d'un calculateur mécanique. Un premier projet voit le jour en 1823, un second, plus élaboré, 10 ans plus tard. C'était un projet visionnaire, ancêtre des ordinateurs modernes, mais

le gouvernement anglais finit par renoncer à subventionner Babbage.

Babbage s'est toujours occupé de cryptographie, déchiffrant de nombreux systèmes différents. En 1854, il reconnaît dans une proposition d'un dentiste de Bristol une variante du système de Vigénère. Le dentiste met Babbage au défi de déchiffrer un texte qu'il a chiffré (un poème) ; il perd, sans que Babbage révèle sa méthode.

En 1863, Friedrich Wilhelm Kasiski (1805-1881), un officier prussien, a la même idée que Babbage ; il est le premier à la publier dans son livre *Die Geheimschriften und die Dechiffrir-Kunst*. Il ne semble pas s'être rendu compte de l'importance de sa découverte.

L'idée est de repérer des répétitions d'une séquence de deux lettres ou plus dans le message chiffré. Une répétition a beaucoup de chances d'indiquer que des séquences identiques du texte en clair ont été codées par des séquences identiques de la clé. Si on repère une répétition dans le message chiffré cela donne donc probablement un multiple de la longueur de la clé. Si on en repère plusieurs, on prend le pgcd des nombres obtenus ; cela donne la longueur de la clé ou un de ses multiples.

Une fois la longueur k de la clé déterminée, on fait des paquets des lettres de k en k. Dans chacun de ces paquets, la lettre la plus fréquente a de fortes chances de chiffrer le e. Cette simple connaissance indique les alphabets choisis pour chiffrer chacun des paquets ; elle donne donc la clé et on en déduit le message originel.

August Kerckhoffs reprend et précise les idées de Kasiski dans son article de février 1883. Il montre comment faire une fois les répétitions relevées ; les analyses de fréquences peuvent être parfois trompeuses, ce dont on s'aperçoit immédiatement par le nombre anormal de lettres rares, K, W... qui apparaissent. Kerckhoffs ajoute que le déchiffrage est plus difficile quand aucune répétition n'a été relevée ; il faut alors tâtonner.

Kerckhoffs aborde ensuite un chiffrement proche de celui du carré de Vigénère : mais au lieu d'utiliser pour chaque lettre du mot clé un alphabet décalé comme l'indique la lettre du mot clé, on utilise un alphabet désordonné ; autrement dit, les lettres du mot clé indexent des bijections de l'alphabet. Dans ce cas, l'observation des répétitions donne la longueur de la clé, mais les fréquences dans les paquets de lettres de k en k ne permettent que de déterminer le chiffrement de la lettre la plus fréquente, le e et d'avoir des points de repère pour les autres. Kerckhoffs donne des conseils : *il faut prendre d'assaut les premiers chiffres de la dépêche*. Savoir le sujet de la dépêche ou la relation entre l'expéditeur et le destinataire deviennent

importants : *la terminaison* ez *est extrêmement rare entre personnes qui se tutoient... la plupart des instructions remises à des inférieurs commencent par* Vous *ou* Le. L'exemple que donne alors Kerckhoffs pour déchiffrer un message où la clé est de longueur 5 est d'une grande virtuosité : il faut repérer des e, examiner un à un tous les mots avec des e aux places trouvées, etc. ; cela ressemble un peu à des mots croisés ou à un scrabble avec des mots courants et des noms propres devinés par la nature du message. Kerckhoffs termine son analyse en expliquant que les bijections choisies ne peuvent l'être totalement au hasard car le chiffrement et le déchiffrement ne doivent pas être trop lents ; pour éviter cette lenteur le système cryptographique ne peut être trop compliqué ; le déchiffreur pourra donc tirer parti de toutes les particularités du chiffrement.

Le commandant Étienne Bazeries raconte comment une répétition de 4 lettres distantes de 21 caractères l'engagea dans une fausse piste dans le déchiffrement d'un télégramme chiffré par la méthode de Beaufort : il fallait tenir compte d'une répétition de 2 lettres distantes de 22 caractères (la clé était la date : *vendredidixseptfévrier* ; choisir une telle clé est dangereux car c'est une clé qu'un déchiffreur peut essayer.

Le commandant Bazeries a souvent utilisé, comme beaucoup d'autres cryptanalistes sans doute, la méthode du mot probable, qui remonte au moins à Porta : on connaît souvent le sujet du télégramme qu'on cherche à déchiffrer ; si c'est un télégramme militaire, on peut supposer rencontrer des mots comme *général, officier, division, attaque, ennemi...*, si c'est un télégramme du monde économique, on peut supposer rencontrer des mots comme *bourse, action, million...*. On place le mot supposé en face d'une suite de lettres du texte chiffré : on détermine les lettres que la clé devrait avoir pour avoir donné le texte chiffré à partir du mot supposé ; en général, cela donne une suite de lettres aléatoires qui ne conviennent pas pour une clé, car les clés sont, à l'époque, des mots ou des groupes de mots choisis pour être facilement retenus sans avoir besoin de les écrire sur un papier. Mais avec un peu de persévérance, il arrive que la méthode donne une suite de lettres vraissemblable. La suite du déchiffrement est alors aisée.

Une dernière méthode est apparue plus tard dans le cas où la méthode des répétitions n'est pas utilisable. On étudie les fréquences des lettres prises de 5 en 5, de 6 en 6, etc. Si le nombre choisi n'est pas égal à la longueur de la clé, les fréquences seront probablement toutes à peu près égales. Si le nombre choisi est égal à la longueur de la clé, le tableau des fréquences sera proche du tableau des fréquences des lettres dans un texte normal et on déterminera

les différents décalages.

Le carré de Vigénère a été aussi utilisé dans la littérature, comme cette lettre de l'un des personnages de la Jangada de Jules Verne, en 1881, chiffrée avec une clé de longueur 6 indiquant des décalages de 4, 3, 2, 5, 1 et 3 lettres.

9.25 Les communications par télégraphe

Pour cette section, mon information principale vient de *Du Morse à l'Internet, 150 ans de télécommunications par câbles sous-marins*, un livre de René Salvador, Gérard Fouchard, Yves Rolland, Alain Paul Leclerc édité par Fouchard et l'Association des amis des câbles sous-marins, livre qui ignore cependant le travail de Gauss et Weber.

Quand Gauss (1777-1855) se lance après la mort de sa seconde épouse, en 1831, dans des recherches de physique sur l'électricité et le magnétisme, il obtient très vite, avec son collègue physicien Wihelm Weber (1804-1891) des résultats fondamentaux. C'est aussi avec Weber qu'il construit le premier télégraphe électromagnétique, en 1833. Ce télégraphe relie l'observatoire et un laboratoire de physique de Göttingen en envoyant des impulsions électriques par un fil ; les déviations de l'aiguille magnétique à l'arrivée codent les lettres du message. Gauss prévoit l'usage du télégrapphe sur de longues distances pour transmettre dans la minute des messages.

Le télégraphe de Samuel Morse (1791-1872) est expérimenté à l'Université de New-York en 1837 ; Morse a l'idée d'un code : son appareil imprime des suites de lignes et de points sur une bande de papier. La France et l'Angleterre refusent de le soutenir. Le Congrès américain lui octroie finalement une subvention pour mettre en service la première ligne commerciale, entre Baltimore et Washington (quelques dizaines de kilomètres), en 1844. Le code Morse est adopté au niveau international en 1855 ; il vient d'être abandonné en 1999.

En quelques années, le télégraphe va transformer la communication des informations dans le monde.

Les premiers câbles sous-marins, très courts, sont posés en 1838. La guttapercha, issue d'un arbre proche de l'hévéa est inventée en 1843. Ses pouvoirs isolants sont étudiés et la production de câbles sous-marins commence en 1848-49.

Le premier câble entre la France et l'Angleterre est posé le 28 août 1850 ; il ne fonctionne que 11 minutes ; celui posé en 1851 fonctionnera plus de 40

ans et l'année suivante, les bourses de Paris et Londres sont reliées entre elles. En France, le réseau télégraphique se développe rapidement sous l'impulsion de Napoléon III. Des câbles sont posés en Méditerranée pour relier la Corse et l'Algérie. Pendant la guerre de Crimée, en août 1855, Napoléon III se rend sur place pour hâter la pose des câbles reliant Paris à Sébastopol par Vienne ; les militaires doivent s'habituer à donner leurs ordres par télégraphe.

Le premier câble reliant l'Irlande à Terre Neuve est posé en août 1858 par deux navires partant du centre de l'Atlantique. La première ligne ne fonctionne que 20 jours, le temps que la reine Victoria et le président Buchanan échangent des salutations. La conception des câbles de grand fond doit encore faire des progrès pour éviter des catastrophes financières. En 1865, une nouvelle tentaive échoue au large de Terre Neuve, mais on réussit à récupérer le câble par 3500 mètres de profondeur et à le réparer. L'année suivante, deux câbles relient l'Europe et l'Amérique du nord ; les débits sont très lents ; le projet de liaison par la Sibérie est abandonné, mais les explorations faites an Alaska ont une conséquence importante : elles révèlent les ressources de cette région et conduisent les Américains à acheter ce territoire au tsar.

Dans les années 1870, des câbles sont posés vers l'Asie, l'Australie, etc. Les Anglais ont un quasi-monopole : 103 000 km de câbles sont anglais sur 118 000 en 1877, 220 000 sur 358 000 en 1901. Les Anglais baissent leurs tarifs (des deux tiers) quand il y a de la concurrence, les relève dès que le câble des concurrents est hors service !

Les utilisateurs du télégraphe sont d'abord les financiers, les diplomates et les militaires. Le réseau international entraîne une augmentation considérable du nombre de messages échangés. La cryptographie est nécessaire pour assurer la confidentialité des messages qui le demandent.

Bien sûr, les messages coûtent chers et des livres d'abréviation sont édités. Par exemple, le code GREEN des USA utilisait des mots codant de cinq lettres, tous formés sur le modèle consonne-voyelle-consonne-voyelle-consonne avec 20 consonnes et six voyelles possibles, ce qui donne $20^3 \times 6^2 = 288\,000$ mots codant possibles. Il ne s'agissait pas de chiffrer des textes, car les codes étaient en vente libre et tout le monde pouvait le faire s'il était pourvu d'un peu de patience ; il s'agissait simplement de réduire le nombre de lettres du message à transmettre afin que le télégramme soit moins coûteux.

Des conférences internationales successives ont fixé les règles de l'usage des réseaux du télégraphe : celle de Londres, entre 20 états, en 1865, est la première ; elle est suivie de bien d'autres, une tous les quatre ans environ. En France, la loi du 13 juin 1866 accorde au public la faculté de correspondre en

chiffres par le télégraphe. Des dispositions spéciales concernaient les dépêches chiffrées : elles interdisaient les longues suites de lettres sans sens, le mélange de chiffres et de lettres dans un même mot et fixaient des règles précises pour déterminer les frais d'envoi.

Si on utilise le télégraphe pour un message chiffré, il faut aussi penser aux erreurs : les télégraphistes risquent sans doute plus de faire des erreurs dans des suites de lettres sans sens que dans les mots de leur langue.

9.26 Auguste Kerckhoffs (1835-1903)

Auguste Kerckhoffs est d'origine hollandaise. Après des études à Liège, il vient enseigner en France, à Melun d'abord. En 1881, il est nommé professeur d'allemand à l'École des Hautes Études et à l'École Arago.

Dans deux fascicules du *Journal des sciences militaires* Auguste Kerckhoffs publie *La cryptographie militaire*, un article en deux parties (janvier 1883, pages 5-38, février 1883, pages 161-191). Le style est clair, direct, précis, concis, polémique et prophétique. Par la suite, Kerckhoffs ne s'occupera plus de cryptographie ; en 1885, il est un des principaux diffuseurs du volapük, une langue à vocation universelle créée en 1879 ; trop complexe, elle cèdera quelques années plus tard devant l'esperanto.

En 1883, l'état de la cryptographie en France est déplorable et les militaires responsables ne se rendent absolument pas compte des problèmes (nous l'avons déjà évoqué). Un général *affirme catégoriquement... que les chiffres à base variables sont illisibles, ou du moins qu'on n'arrive à les déchiffrer qu'avec des difficultés inouies*, alors qu'on souligne en Allemagne que la cryptographie est un *auxiliaire puissant de la tactique militaire* et *doit être employée de la manière la plus étendue*. Par exemple, en 1871, les Allemands ont profité de ce que les communications entre les assiégés parisiens et les armées de province n'étaient pas chiffrées solidement.

Kerckhoffs veut exposer *un état des choses ... dont nos ennemis du dehors ne pourraient un jour que trop bien et trop aisément tirer parti*. Citant un général, il ajoute qu'*il faudrait durant la paix exercer nos officiers à cette correspondance... D'ailleurs, même en paix, on a besoin à chaque instant de correspondre secrètement*.

Kerckhoffs commence en énonçant des principes de base auxquels doit satisfaire tout système de cryptographie destiné à des échanges entre militaires. Ces principes sont toujours cités aujourd'hui.

Kerckhoffs souligne d'abord que le système employé doit être stable, qu'il ne doit pas être modifié au gré de l'un des utilisateurs, qu'il ne doit pas nécessiter de garder avec soi quelque chose *qui soit de nature à éclairer l'ennemi sur le sens des dépêches secrètes qui pourraient tomber entre ses mains.* Il énonce ensuite les six principes de base qu'un système cryptographique doit satisfaire.

1) *Le système doit être matériellement, sinon mathématiquement, indéchiffrable.*

2) *Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi.*

3) *La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants.*

4) *Il faut qu'il soit applicable à la correspondance télégraphique.*

5) *Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes.*

6) *Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.*

Si les conditions 4-5-6 ne lui semblent pas poser de difficulté, Kerckhoffs insiste sur les premiers points.

Pour le 1, certains pensent qu'un système qui résiste quelques heures suffit aux militaires car les nouvelles chiffrées perdent leur intérêt au bout de trois-quatre heures. Lui explique que c'est loin d'être toujours la cas, citant l'exemple du commandant d'une place assiégée en communication avec l'armée qui doit la secourir. Il ajoute qu'une fois qu'un texte chiffré a été déchiffré, l'ennemi pourra déchiffrer instantanément toutes les dépêches suivantes utilisant la même clé.

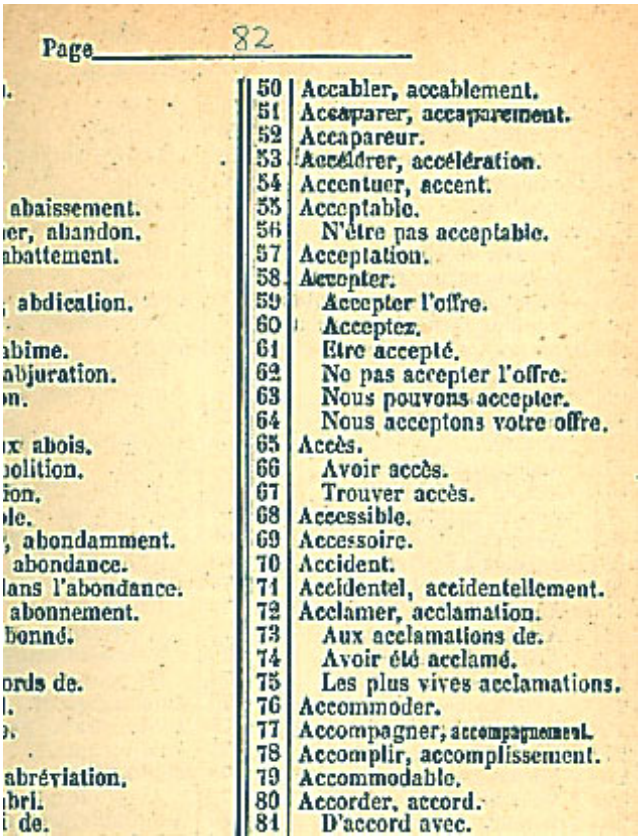
Pour le 2, Kerckhoffs condamne l'emploi du dictionnaire dans l'armée : si trop de gens partagent le secret, le danger est évident. Il plaide pour un système enseigné au grand jour, que nos voisins pourraient connaître et même copier ; la méthode serait alors reconnue comme efficace par le plus grand nombre et le secret résiderait dans la clef.

9.27 Les répertoires vers 1880-90

L'usage des répertoires s'est développé depuis les Rossignol. Des phrases entières étaient parfois associées à un nombre. Elles étaient évidemment indéchiffrables, mais le système était d'une grande fragilité par ailleurs. Vers

1850, on pense à composer des dictionnaires pour le public ; plusieurs sont pub liés à la fin du dix-neuvième siècle ; ils connai !ssent de nombreuses éditions.

Le *Code télégraphique chiffré* de F.-G. Sittler comptera de nombreuses éditions.



Page 82

	50	Accabler, accablement.
	51	Accaparer, accaparement.
	52	Accapareur.
	53	Accélérer, accélération.
abaissement.	54	Accentuer, accent.
ıer, abandon.	55	Acceptable.
ıbattement.	56	N'être pas acceptable.
	57	Acceptation.
abdication.	58	Accepter.
	59	Accepter l'offre.
	60	Acceptez.
ıbîme.	61	Etre accepté.
abjuration.	62	Ne pas accepter l'offre.
ın.	63	Nous pouvons accepter.
	64	Nous acceptons votre offre.
ıx abois.	65	Accès.
ıolition.	66	Avoir accès.
ion.	67	Trouver accès.
ıle.	68	Accessible.
abondamment.	69	Accessoire.
abondance.	70	Accident.
lans l'abondance.	71	Accidentel, accidentellement.
abonnement.	72	Acclamer, acclamation.
ıonné.	73	Aux acclamations de.
	74	Avoir été acclamé.
ords de.	75	Les plus vives acclamations.
ı.	76	Accommoder.
ı.	77	Accompagner, accompagnement.
	78	Accomplir, accomplissement.
abréviation.	79	Accommodable.
ıbri.	80	Accorder, accord.
i de.	81	D'accord avec.

Une page du Code télégraphique chiffré de Sittler.

L'usage du livre était simple : on indiquait au correspondant les numéros de page et de ligne des mots ou phrases de son message les uns après les autres, ce qui donnait des groupes de quatre chiffres. On pouvait convenir d'énumérer ces quatre chiffres dans un des 24 ordres possibles, voire leur ajouter ou leur retrancher 1, par exemple, pour rendre le déchiffrement un peu plus difficile. La conjugaison des verbes était indiquée par l'infinitif suivi, par exemple, de *futur*. Les noms propres étaient syllabés.

9.28 L'affaire Dreyfus et le télégramme de Panizzardi

[3]Le 15 octobre 1894, un conseil d'officiers arrête le capitaine Alfred Dreyfus : son écriture présentait des similitudes avec celle d'un bordereau livrant à l'Allemagne des informations confidentielles. Le 1er novembre la presse révèle l'affaire : *La Libre Parole* indique que Dreyfus est à la solde de l'Allemagne ou de l'Italie. L'attaché militaire italien, Alessandro Panizzardi, écrivit à Rome que ni lui ni son collègue allemand ne connaissaient Dreyfus. Le lendemain 2 novembre, il envoya un télégramme chiffré demandant qu'un démenti officiel soit publié si aucun contact avec Dreyfus n'avait eu lieu.

Le texte en clair du télégramme était le suivant :

Si le capitaine Dreyfus n'a pas eu de relations avec nous, il serait bon de faire publier par l'ambassadeur un démenti officiel pour éviter les commentaires de la presse.

Il innocentait totalement Dreyfus.

Mais l'histoire est pleine d'aléas. Le télégramme était codé avec le code Baravelli, un code commercial publié au début de l'année à Turin. Le code comportait 100 pages consacrées au vocabulaire, numérotées par deux chiffres, de 00 à 99, et comportant 100 mots. Il comportait aussi des pages pour les syllabes, les formes grammaticales, les consonnes et chacun pouvait convenir de sa propre numérotation des pages.

L'exemple donné dans le livre de Kahn, page 78, est celui de la page numérotée 75 du code. Elle contient d'abord une ligne où on peut indiquer un autre numéro pour cette page. Puis elle donne cent noms numérotés de 00 à 99 et classés par ordre alphabétique ; parmi eux :

01 pour Razional, 05 pour Il Re di, 06 pour S.M. il Re, 53 pour Reggio Calabria, 54 pour Reggio Emilia, 77 pour Reichstag, 78 pour Reichsmark, 93 pour Religione.

Les services français possédaient un exemplaire du code, pour avoir suivi une intrigue amoureuse entre le comte de Turin, neveu du Roi d'Italie et la Duchesse Grazioli habitant l'hôtel de Windsor : un agent français avait réussi à voler un exemplaire du code dans la chambre de la Duchesse sous une pile de mouchoirs.

Le message codé intercepté par les services français était le suivant :

3. [KAH], pages 76-84

913 44 7836 527 3 88 706
6458 71 18 0288 5715 3716
7567 7943 2107 0018 7606 4891
6165

C'était la première fois que Panizzardi utilisait le code Baravelli. Supposant que le nom de Dreyfus figurait dans le télégramme et qu'il avait été codé sous la forme *Dr-e-y-fus*, les déchiffreurs français trouvèrent dans le code *dr* à la ligne 27 de la page 2, *e* à la ligne 1 de la page 1, *fus* à la ligne 06 de la page 3, *y* à la ligne 8 de la série 9. Une séquence du télégramme avait une forme semblable à ce qu'on pouvait attendre : 227 1 98 306 ; c'était 527 3 88 706, ce qui indiquait des changements de pagination de trois des quatre morceaux de Dreyfus opérés par les services italiens.

A partir de là, un premier texte fut transmis aux Services français ; la fin du décryptage était erroné et pouvait se lire comme une confirmation de la culpabilité de Dreyfus. Quand la version finale et exacte du télégramme fut au point, le 10 novembre, les services français hésitèrent à revenir sur leur interprétation. Ils eurent l'idée de fabriquer un faux message indiquant que les services français allaient recevoir des documents sur le plan de mobilisation italien ; ils y placèrent des mots (noms de personne, adresse) qui devaient leur permettre de détermination la pagination exacte du code Baravelli utilisée par les diplomates italiens. Les français avaient prévus que Panizzardi, allait informer ses supérieurs de toute urgence de ce télégramme qu'il jugerait important en le recopiant mot pour mot et qu'il leur enverrait une copie de leur message codé. C'est ce qui arriva. Les services français interceptèrent le second télégramme de Panizzardi, le firent décrypter. Le texte avait été prévu pour lever les difficultés de décodage du premier télégramme de Panizzardi et le décryptage se révéla correspondre exactement au texte initial. Cette méthode de faire diffuser par l'ennemi des textes est redoutablement efficace ; le second télégramme Panizzardi en est un exemple.

Le décryptage du premier télégramme de Panizzardi était donc correct, ce qui prouvait l'innocence de Dreyfus. Mais les officiers français, qui jugeait que le télégramme était le pivot de l'affaire, s'arrangèrent pour jeter le doute : il y avait eu plusieurs versions contradictoires, etc. et une version fausse, soit-disant dictée de mémoire, accusait Dreyfus. Le texte correct ne fut joint au dossier que durant le procès en cassation, le 27 avril 1999. La réhabilitation de Dreyfus était en chemin, mais encore lointaine.

9.29 Tannenberg, catastrophe cryptographique

Au début de la guerre, les Russes attaque la Prusse orientale. Deux grandes armées font mouvement vers Könisberg, la ville de Prusse orientale du grand Hilbert et des ponts d'Euler dont il ne reste rien aujourd'hui. La première armée est au nord des lacs Mazure sous les ordres du général de Rennenkampf, la seconde armée est au sud des lacs et remonte vers le nord sous les ordres du général Samsonov. Les deux armées russes comptent 400 000 hommes, deux fois plus que les armées allemandes (une grande partie des armées allemandes est concentrée sur le front ouest où va avoir lieu la première bataille de la Marne, début septembre 1914). Les armées russes cherchent à prendre en tenailles les armées allemandes et remporte une première victoire à Gumbinnen (20 août). Pour se renforcer, les Allemands doivent retirer deux corps d'armée engagés à l'ouest.

Les Russes sont alors en position de force, mais leur organisation est désastreuse. Ils n'ont pas de rations, pas de munitions, pas de câble pour assurer les liaisons ; les systèmes de chiffrage qu'ils utilisent pour chiffrer leurs communications ne sont pas compatibles : une armée possède un nouveau système et a jeté l'ancien, une autre n'a que l'ancien. Vers le milieu du mois d'août, les armées russes ne peuvent plus échanger d'informations qu'en clair, par les quelques radios de campagne dont disposent leurs généraux ; les officiers russes affirment d'ailleurs qu'il n'y a aucune raison de se compliquer l'existence en chiffrant les messages, que les Allemands ne restent sûrement pas 24 heures sur 24 à écouter leurs radios...

C'était d'une imprudence extrême. Les Allemands sont stupéfaits d'entendre Rennenkampf expliquer à Samsonov qu'il avance lentement sans effectuer la tenaille prévue. Hindenburg, qui était à la retraite, vient juste d'être rappelé le 22 août pour diriger le front est. Conseillé par le général Luddendorf (trop jeune pour qu'on lui confie le commandement) et le colonel Hoffmann, il déplace les troupes du nord par chemin de fer, attaque l'armée de Samsonov et l'anéantit en trois jours (30 000 morts, près de 100 000 prisonniers, Samsonov se suicide) ; puis il se retourne vers l'armée du nord.

C'est Hindenburg qui recueille les fruits de cette victoire et sa popularité est immense. Il choisit le 29 août de donner le nom de victoire de Tannenberg à cette bataille : il efface ainsi le souvenir de la défaite écrasante subie le 15 juillet 1410 par les troupes de l'Ordre Teutonique devant une armée commandée par Ladislav II Jagellon, prince lithuanien devenu roi de Pologne en

1386.

Les semaines qui suivent montrent les Allemands, avec leurs alliés austro-hongrois, réussissant à percer les procédés cryptographiques des Russes presque sans discontinuer et manœuvrer en ayant une connaissance parfaite des mouvements et des positions de leurs ennemis, remportant succès sur succès.

L'échec des services cryptographiques russes est encore plus évident en 1915. Le transport des clés dans une armée désorganisée se révèle impossible. Le système de chiffrement le plus fréquemment utilisé est une sorte de système de Jules César très facile à déchiffrer. Ainsi, les Russes allaient de défaite en défaite, suivant un chemin qui les conduisaient aux soubresauts de 1918 : le succès de Lénine et des bolcheviks s'expliquerait par une extraordinaire défaillance cryptographique !

9.30 George Painvin (1886-1980)

George Painvin entre major à l'école polytechnique en 1905 ; son père, son grand-père, son frère, son beau père sont passés par là. Il poursuit par l'École des mines et devient professeur de géologie, paléontologie et chimie.

En 1914, le capitaine Paulier lui fait découvrir la cryptographie pour laquelle il se passionne. Ses premiers succès le font affecter au Cabinet noir de l'état-major de l'armée à Paris. Dans un document de 1921, Painvin donne un aperçu de l'ampleur de ses travaux déchiffrement des systèmes de chiffrement allemands ; il énumère une vingtaine de système différents dont il a compris le fonctionnement. Son travail consistait également à comprendre

les variantes introduites et à rétablir les clés utilisées par les Allemands et changées régulièrement. À partir de 1917, six personnes aident Painvin. Le plus célèbre succès de Painvin est d'avoir permis le déchiffrement du *Radiogramme de la victoire* dont je vais parler plus loin.

Après la guerre, Painvin travaille dans la chimie, crée la Chambre syndicale de la Grande industrie chimique, préside l'Union des industries chimiques, puis la Société de chimie industrielle et la Chambre de commerce de Paris.

Il peut enfin parler de ses activités de cryptographe dans les années 1960, le secret militaire ne lui tant plus imposé.

9.31 ADFVX et ADFGVX

Les militaires français ont eu un avantage que la guerre se déroule en France. Leurs télégrammes étaient transmis par des réseaux filaires mis en place depuis des années ; les Allemands ne pouvaient pas les intercepter. Les télégrammes allemands étaient envoyés par radio et pouvaient être captés par des stations d'écoute dont les performances étaient constamment améliorées.

Un nouveau code est introduit par l'armée allemande le 5 mars 1918. Il est dû à un spécialiste allemand de 27 ans, Fritz Nebel. Subitement, les cryptographes français sont incapables de déchiffrer les messages allemands. Le changement de système de chiffrement pouvait être interprété comme un signe fort : il s'agissait de dérouter les services français et de les empêcher de suivre les préparatifs et les développements d'une nouvelle offensive.

Les messages ne comportant que les cinq lettres ADFVX. Ces lettres ont été choisies par Nebel parce que leurs codages bien distincts en morse permettaient facilement, en cas d'erreur dans la saisie ou de lacune dans la transmission par des recrues inexpérimentées, de corriger le texte reçu et qu'il avait réalisé que, comme $5 \times 5 = 25$, les couples de lettres de ADFVX pouvaient coder 25 lettres de l'alphabet. Le codage morse des lettres du code est :

A : .−
D : −...
F : .. − .
G : − − .
V : ...−
X : −..−

Painvin pense que le chiffrage est basé sur une grille carrée de 5 par 5 où 25 lettres de l'alphabet sont codées par des couples de lettres de l'ensemble {A,D,F,V,X} et que ce premier chiffrage est suivi d'un second, une transposition, chacun ayant leur clé. Nous décrirons en détail ces procédés plus loin. Mais le nombre de messages captés est faible et les cryptographes français sont seulement capables de supposer un changement de clés, les fréquences des cinq lettres variant d'un jour à l'autre. L'offensive allemande pouvait donc se préparer et se déclencher avec l'effet de surprise recherché.

La Russie a cessé la guerre avec l'Allemagne (un armistice a été signé à Brest-Litovsk le 15 décembre 1917 et la paix est signée dans la même ville le 3 mars 1918). En ce début de 1918, la situation militaire est en train de changer rapidement. D'une part, les Allemands ont pu redéployer leurs troupes du front oriental sur le front au nord de la France. D'autre part, les troupes américaines arrivent depuis la fin de 1917 [4].

Pendant quelques heures, Painvin et ses collaborateurs ont un autre sujet de recherche, car les Allemands mettent en service le 11 mars 1918 à minuit 40 un autre système de chiffrage, le Schlüsselheft. Le premier message envoyé n'est pas compris de la station destinataire : *Ohne Sinne*, sans signification, répond-elle, demandant que le message lui soit transmis en ancien code. Les services français disposent alors de deux versions du même message, l'une dans un code qu'elles savent déchiffrer, l'autre dans un code nouveau : le déchiffrage fut alors aisé.

La grande offensive allemande est déclenchée le 21 mars à 4 heures 30. L'augmentation du trafic en ADFVX qui en résulte permet aux Français, en analysant les fréquences des cinq lettres, de comprendre que les Allemands changent leurs clés tous les jours.

Cette histoire m'a permis de replacer un événement personnel dans un contexte plus significatif. Le 23 mars 1918, entre Guiscard et Fréniche au nord de Noyon, mon père est blessé juste au-dessus du poumon gauche ; à quelques centimètres près, je ne serais pas devant mon ordinateur aujourd'hui.

Le premier avril, 18 messages en ADFVX sont captés, comptant 512 groupes de 5 lettres. Le 4 avril, Painvin remarque que deux de ces messages commencent par les mêmes séquences ; il suppose que les textes en clair ont des débuts identiques et parvient en deux jours au premier déchiffrement. Painvin reprend alors les messages du 29 mars qui sont assez nombreux. Il

4. Pour l'entrée en guerre des Etats-Unis, le télégramme Zimmermann est d'une grande importance.

réussit le 26 avril à en reconstituer les clés. Ses méthodes s'améliorent : il trouve en deux jours les clés des messages du 28 mai et en moins d'une journée celles des messages du 30 mai.

Deux événements simultanés font craindre le pire aux alliés. Sur le plan militaire, Luddendorff a lancé le 27 mai à une heure du matin une offensive puissante au Chemin des Dames qui prend les troupes françaises et anglaises par surprise. Les lignes françaises sont enfoncées, le plateau du Chemin des Dames est occupé à cinq heures et à 10 heures les Allemands arrivent sur les bords de l'Aisne. Le lendemain soir, les Allemands pénètrent à Soissons et, trois jours plus tard, ils sont à Chateau-Thierry, sur les bords de la Marne à 85 km de Paris, comme en 1914. Sur le plan cryptographique, c'est une catastrophe : le premier juin, le système ADFVX est subitement remplacé par un nouveau système où apparaissent les six lettres ADFGVX.

Painvin s'attaque aux télégrammes du premier juin dans la soirée. Il pense que le nouveau système est une évolution du système ADFVX avec une grille de six par six codant les 26 lettres et les 10 chiffres par des couples d'éléments utilisant les six lettres. Il est servi par la chance : il remarque que trois télégrammes ont été envoyés à la même heure, minuit cinq, de la même station et commence leur étude. Deux d'entre eux ont 106 caractères et Painvin peut en déduire la longueur de la clé. Le troisième a 108 caractères et Painvin suppose qu'il s'agit du même texte avec un décalage dû au nom du destinataire. Il réussit à reconstituer la clé et la grille le 2 juin à 19 heures.

Sur le terrain, l'offensive de Luddendorf était provisoirement contenue, mais les canons allemands à longue portée bombardaient Paris. La ligne de front n'avait plus la régularité qu'elle avait en mars. Des portions entières avaient été enfoncées, d'autres avaient tenu et constituaient ce qu'on appelait des saillants.

Le matin du 3 juin, avec les clés trouvées par Painvin, les services français déchiffrèrent un message allemand adressé à la $18^{\text{Øme}}$ armée allemande à Remaugies, au nord d'un saillant :

Munitionierung beschleunigen Punkt soweit nicut eingesehen auch bei Tag dont la traduction, compte tenu de l'erreur de transmission nicut = nicht, est :

Accélérer le ravitaillement en munitions, même de jour, à condition de ne pas être vu.

Le capitaine Guitard comprit l'importance de ce message : il signifiait qu'une attaque était imminente dans ce secteur et que les Allemands devant faire vite, allaient acheminer des munitions de jour (jusqu'ici, Luddendorf

avait pu acheminer les munitions de nuit, privant les alliés d'indices pour déterminer le lieu de ses attaques ; mais les difficultés de l'organisation de sa grande offensive le contraignaient à enfreindre ses règles).

Les observations aériennes permirent de vérifier cette hypothèse, des déserteurs annoncèrent l'attaque pour le 7 juin. Foch prépara ses troupes pour cette bataille, dégarnissant les avant-postes. Luddendorf repoussa l'attaque de deux jours pour réunir toute la puissance de feu nécessaire. Mais après cinq jours de durs combats, il dut reculer pour la première fois depuis deux mois. Les combats des mois suivants furent acharnés, mais les troupes allemandes durent reculer. La seconde bataille de la Marne commence le 18 juillet, puis les offensives alliées se multiplient. Le Chemin des Dames est repris le 10 octobre, Guillaume II est contraint d'abdiquer le 9 novembre, l'armistice est signé à Rethondes le 11 novembre, sans que la guerre ait été portée sur le sol allemand.

La cryptographie, et Painvin en particulier, avaient joué un rôle dont l'importance est difficile à évaluer dans cet épisode de la guerre. Pendant 30

ans, le secret militaire a ; s'agit-il vraiment du *Radiogramme de la victoire* comme beaucoup l'ont dit ? La question est la même pour le rôle de Painvin et des cryptographes français durant toute la guerre, de 1914 à 1918. Mais combien de millions de morts pendant ces quatre années ?

Quand à Painvin, son travail mené nuit et jours pendant ce printemps l'avait exténué et il fut mis quelques temps au repos.

9.32 Le *Radiogramme de la victoire*

Sophie de Lastour donne les clés du chiffrement du *Radiogramme de la victoire*.

La grille du chiffrement était la suivante.

	A	D	F	G	V	X
A	c	o	8	x	f	4
D	m	k	3	a	z	9
F	n	w	l	0	j	d
G	5	s	i	y	h	u
V	p	l	v	b	6	r
X	e	q	7	t	2	g

Le message *Munitionierung beschleunigen Punkt soweit nicut eingesehen auch bei Tag* se chiffre donc par :

DA GX FA GF XG GF AD FA GF XA VX
GX FA XX VG XA GD AA GV FF XA GX
FA GF XX XA FA VA GX FA DD XG GD
AD FD XA GF XG FA GF AA GX XG XA
GF FA XX XA GD XA GV XA FA DG GX
AA GV VG XA GF XG DG XX

Sophie de Lastours corrige le message en écrivant *nicht* : on comprend mieux l'erreur sur ce mot en remarquant que h et u occupent des cases contiguës dans la grille.

La clé de transposition était de longueur 21. On écrivait donc le message par séquences de 21 caractères placés sous la clé de la façon suivante. Dans ce cas particulier, la longueur du message était un multiple de la longueur

de la clé.

6	16	7	5	17	2	14	10	15	9	13	1	21	12	4	8	19	3	11	20	18
D	A	G	X	F	A	G	F	X	G	G	F	A	D	F	A	G	F	X	A	V
X	G	X	F	A	X	X	V	G	X	A	G	D	A	A	G	V	F	F	X	A
G	X	F	A	G	F	X	X	X	A	F	A	V	A	G	X	F	A	D	D	X
G	G	D	A	D	F	D	X	A	G	F	X	G	F	A	G	F	A	A	G	X
X	G	X	A	G	F	F	A	X	X	X	A	G	D	X	A	G	V	X	A	F
A	D	G	G	X	A	A	G	V	V	G	X	A	G	F	X	G	D	G	X	X

Il reste à disposer les lettres de ce tableau par groupe de cinq horizontalement : on prend verticalement les lettres des colonnes, dans l'ordre des colonnes, ce qui donne le texte suivant.

FGAXA XAXFF FAFFA AVDFA GAXFX
FAAAG DXGGX AGXFD XGAGX GAXGX
AGXVF VXXAG XFDAX GDAAF DGGAF
FXGGX XDFAX GXAXV AGXGG DFAGD
GXVAX XFXGV FFGGA XDGAX ADVGG
A

Notons que les transpositions étaient depuis longtemps courantes dans le monde de la cryptographie ; elles se décèlent facilement car les différentes lettres de l'alphabet conservent leurs fréquences habituelles. Une fois qu'on a deviné qu'un texte est codé par transposition, il reste à déterminer la longueur de la clef et la permutation des colonnes utilisée : c'est affaire de tâtonnement et d'expérience (penser au Q toujours suivi d'un U, au X souvent précédé d'un U, etc. Une transposition sur les colonnes pouvait être suivie d'une transposition sur les lignes comme dans le système des nihilistes russes

9.33 La seconde défaite de Nebel

L'épilogue de l'histoire est assez émouvante. Sophie de Lastours raconte longuement comment, en 1968, une rencontre entre Georpes Painvin et Fritz Nebel (que de nombreux sites donnent mort en 1967) fut organisée au Cercle suédois, à Paris ; 50 ans s'étaient passés depuis les célèbres déchiffrements de Painvin, mais rien n'avait été publié sur le détail de sa réussite jusque là pour cause de secret militaire ; il y avait eu cependant des articles et des conférences où le *radiogramme de la victoire* était évoqué).

Nebel ne pensait pas que les codes qu'il avait inventés avaient été percés à ce point et Painvin lui révèle le détail de ses analyses ; il lui apprend aussi le hasard des télégrammes de 106-106 et 108 lettres envoyés simultanément. Nebel était paraît-il extraordinairement troublé et accablé en écoutant les explications précises de Painvin qui les unes après les autres établissaient de plus en plus nettement, cinquante années après, comment la défaite allemande était liée à sa défaite cryptographique !

Painvin imagine que Nebel aurait pu introduire des couches nouvelles de difficulté mais que cela aurait rendu le système trop délicat pour les chiffreurs. Il remercie finalement Nebel d'avoir construit ses systèmes ; pour lui qui aimait les défis, il en avait rencontré un vraiment intéressant et avait poursuivi sa solution avec un acharnement extraordinaire.

Chapitre 10

Mathématiques du monde arabe

10.1 Le monde arabe

Mahomet (570-632) naît à La Mecque, une cité situé sur la route des caravanes d'Aden vers le nord. On a beaucoup de renseignements sur sa vie, recueillis longtemps après les événements, mais soumis à l'époque à un examen critique. Il a 25 ans quand il épouse Khadidja, une riche veuve de 15 ans son aînée au service de laquelle il était berger.

C'est en 610 que commencent les apparitions de Gabriel et que Mahomet commence à enseigner oralement à ceux qui deviendront les musulmans, ceux qui se soumettent à Dieu. Il commence à avoir des disciples et les habitants de La Mecque le chassent en 622. Il se réfugie à Yatrib qui change de nom et devient Médine (la ville) où il a de nombreux partisans. Le Ramadan se met en place. Son armée lutte contre celle des Mecquois. Les Mecquois font sans succès le siège de Médine en 628 ; Mahomet marche sur La Mecque en 630 et la prend sans effusion de sang. Il meurt en 632.

Pour ses successeurs, les califes, commencent les grandes périodes de conquête et d'assassinats mutuels : Abu Bakr (mort en 634) est suivi de Omar. Uthman est assassiné en 656. Ali, le gendre de Mahomet en 661 et l'opposition entre sunnites (Sunna : la tradition du prophète) et chiites (le parti d'Ali) commençait. Le Coran est fixé dans les années 650.

En 711, les troupes arabes traversent le détroit de Gibraltar (djebel de Tarik ibn Ziyad, leur commandant). Elles sont stoppées en France dans les

années 730 (la bataille de Poitiers a lieu en 732).

L'empire arabe connaît un développement culturel et scientifique considérable sous les règnes des califes Haroun al Rachid (786-809) et al Mamoun (813-833). Le Bayt al Hikma, la Maison de la sagesse [1], réunit des savants d'origines et de cultures diverses ; ils rassemblent les connaissances de leur époque, se procurent des manuscrits grecs. Les années 800 sont la grande époque des traductions : Euclide (trois fois), Ptolémée (deux fois), Archimède, Apollonius, Diophante, les mathématiciens indiens, etc. Puis les sciences arabes connaissent un développement extraordinaire [2]. Dans les années 1100, la reconquête de l'Espagne a commencé. Les érudits du monde chrétien se précipitent à Tolède [3], ville contact entre le monde chrétien et le monde musulman, pour y traduire des dizaines de manuscrits arabes, certains étant des traductions de textes grecs ; parmi les 80 (environ) ouvrages traduits par Gérard de Crémone (vers 1114-1187) et son atelier figurent l'Almageste de Ptolémée, des traités d'Aristote et d'Apollonius, aussi bien que des textes d'auteurs arabes ; Adélard de Bath (vers 1075-1160) traduit les Éléments d'Euclide, etc.

10.2 Al Khwarizmi (vers 790-840/850)

Le nom de Mohammed ibn Musa al Khwarizmi (Mohammed fils de Moïse) semble indiquer qu'il était originaire du Khwarezm, une province de l'Ouzbékistan.

Le principal ouvrage mathématique d'Al Khwarizmi est Al Kitab al Mukhtasar fi Hisab al jabr wa-l-Muqabala : *Livre concis du calcul par les procédés du jabr et du muqabala* (merci de m'excuser pour l'orthographe arabe imparfaite). Il a été traduit par Robert de Chester [4] à Ségovie en 1145 ; en 1831, Frederic Rosen en a publié une copie de 1342. Rédigé à l'époque d'al Ma-

1. Cette institution a été recréé récemment.

2. Voir les trois volumes de *Histoire des sciences arabes*, publiés sous la direction de Roshdi Rashed au Seuil en 1997 : vol. 1 : *Astronomie théorique et appliquée*, vol. 2 : *Mathématiques et physique*, vol. 3 : *Technologie, alchimie et sciences de la vie*. Voir aussi : Youschkevitch Adolf, *Les mathématiques arabes*, Vrin, 1976. Voir aussi : Djebbar Ahmed, *Histoire de la science arabe*, Seuil, 2001.

3. *Je me hâtai de m'y rendre pour écouter les leçons des plus grands savants du monde* écrit Robert de Morlay.

4. Robert de Chester venait de traduire le Coran, en 1141, avec deux autres chrétiens et un arabe, à la demande de Pierre le Vénérable, le grand abbé de Cluny dont le but était de faire connaître aux chrétiens la religion qu'il voulait combattre.

moun, l'ouvrage traite des équations du second degré liant les dirhams, les racines et les carrés (correspondant à nos nombres, nos x et nos x^2). Al Khwarizmi a l'idée de les classer en six types différents, toujours en phrases : *Racines et carrés égaux à des nombres*, *Carrés et nombres égaux à des racines*, *Racines et nombres égaux à des carrés*, autrement dit $ax^2 + bx = c$, $ax^2 + c = bx$, $bx + c = ax^2$ avec $a, b, c > 0$ [5]. Il montre comment les résoudre sur les exemples : $x^2 + 10x = 39$, $x^2 + 21 = 10x$, $3x + 4 = x^2$ (il préfère toujours se ramener au cas où $a = 1$), puis traite une trentaine d'équations comportant des difficultés de calcul diverses. Au lecteur de comprendre comment traiter d'autres exemples à partir de ceux-ci, mais tout ce qui relève de l'algèbre *doit te mener à l'un des six types que j'ai décrits dans mon livre.* Pour le premier et le troisième exemple, il donne une résolution identique à la babylonienne (2500 ans avant lui), indiquant la méthode de calcul de la racine positive. Pour le second, il innove.

Divise[6] *en deux les racines ; ce qui donne 5 ; multiplie 5 par lui-même, tu obtiens 25 ; retire les 21 qui sont ajoutés au carré ; il reste 4 ; extrais la racine, cela donne 2, et retire-la de la moitié de la racine, c'est-à-dire de 5 ; il reste 3 ; c'est la racine du carré que tu cherches et le carré est 9. Si tu le désires, ajoute cela à la moitié de la racine, ce qui donne 7, qui est la racine du carré que tu cherches et le carré est 49. Si tu rencontres un problème qui se ramène à ce cas, examine alors sa justesse à l'aide de l'addition ; si tu ne le peux, tu obtiendras certainement (la solution) à l'aide de la soustraction. Parmi les trois cas dans lesquels on doit diviser en deux les racines, c'est le seul où l'on se serve de l'addition et de la soustraction. Sache en outre que si, dans ce cas, tu divises en deux la racine, que tu la multiplies par elle-même et que le produit soit plus petit que les dirhams qui sont ajoutés au carré, alors le problème est impossible. Mais s'il est égal aux dirhams, la racine du carré est égale à la moitié de la racine, sans qu'on ajoute ou retire quoi que ce soit.*

Autrement dit, Al Khwarizmi explique que, dans un problème du type $x^2 + c = bx$, si $(\frac{b}{2})^2 < c$, alors le problème est impossible et si $(\frac{b}{2})^2 = c$, alors la solution est $\frac{b}{2}$, sans addition ni soustraction.

Il faut souligner l'importance de cette partie du travail d'Al Khwarizmi : c'est la première fois qu'on considère qu'une équation du second degré peut

5. Les trois autres types sont plus faciles : $ax = b$, $ax^2 = b$, $ax^2 = bx$.
6. Traduction d'après Youschkevitch.

avoir deux racines ; le critère d'existence à l'aide du discriminant de l'équation est donné.

Un autre aspect du travail d'al Khwarizmi sur les équations mérite d'être rapporté : pour chacune, il donne une justification géométrique de sa démarche. L'exemple le plus simple est celui des équations comme $x^2 + 10x = 39$ (on remarquera que la figure ne permet pas de construire un segment de longueur x, c'est juste une figure pour expliquer la marche des calculs).

Al Khwarizmi considère un carré de côté x et donc d'aire x^2. Les $10x$ sont interprétés comme l'aire de deux rectangles de côtés x et $5 = 10/2$ (autrement dit le coefficient de x divisé par 2) adjoints au carré. L'aire de la surface ainsi obtenue doit être 39. En ajoutant à cette surface d'aire 39, un carré de côté 5 situé au coin de la figure, on obtient un nouveau carré de côté $x+5$ et d'aire $(x+5)^2$, d'où $(x+5)^2 = 39 + 25 = 64$, etc. La géométrie n'a pas servi ici à construire un segment de longueur égale à une racine de l'équation, mais à justifier ce qui correspond à la mise du trinôme sous forme canonique.

Pour nous, cette résolution est incomplète car, si $(x+5)^2 = 64 = 8^2$, on a $x + 5 = 8$ ou $x + 5 = -8$, donc $x = 3$ ou $x = -13$. Mais à l'époque d'al Khwarizmi, on ne considérait que les racines positives des équations (les nombres négatifs ne sont devenus usuels que « récemment », depuis 200 à 300 ans).

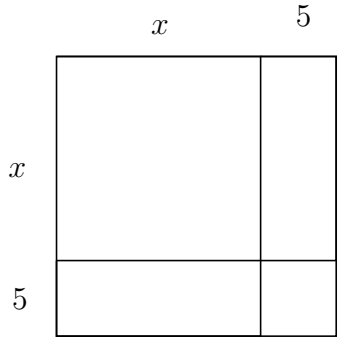


Figure 16

Al Khwarizmi passe de l'équation :

$$4x^2 - 2x + 3 = 3x^2 + 2$$

à l'équation

$$4x^2 + 3 = 3x^2 + 2x + 2$$

par *al jabr*, mot qui exprime, en arabe, l'idée de remplissage ou de réduction d'une fracture. C'est l'opération consistant à ajouter aux deux membres d'une équation le même terme afin de faire disparaître les termes affectés du signe $-$. Ce mot est à l'origine du mot algèbre, ayant été conservé tel quel dans les premières traductions latines.

Un ouvrage probablement ultérieur d'Al Khwarizmi explique, pour le monde arabe, les méthodes indiennes de calcul [7] ; il traite d'arithmétique élémentaire, contient un premier exposé du système décimal et explique l'usage d'un petit cercle pour noter l'absence d'unités, de dizaines, de centaines... transmettant ainsi l'invention indienne du zéro : al Khwarizmi explique que les Indiens, ne voulant pas confondre les écritures de 1 et 10 ont marqué à la droite du 1 un petit cercle et de même pour écrire, vingt, trente, etc. ; pour écrire 100, il faudra placer deux petits cercles, pour écrire 307, il faudra placer un petit cercle entre le 3 et le 7, etc. A partir de 1150, ce livre est à son tour traduit en latin à de très nombreuses reprises et diffusé dans toute l'Europe par des manuscrits appelés *algorismus*, déformation d'Al Khwarizmi, mot qui donne algorithme et a pris le sens de *procédé de calcul* que l'on sait. Le signe rond est alors appelé circulus ou cifre, transcription de l'arabe as-sifr. Le mot deviendra chiffre en français, zéro en italien. Attention, ce signe rond est un signe d'absence et non le signe représentant le nombre 0 dont Brahmagupta avait énoncé les propriétés.

10.3 Omar Khayyam (1048-1131)

Omar Khayyam est astronome, mathématicien, philosophe. La date de sa naissance, la date de sa mort sont données par des documents uniques : son horoscope, un témoignage. Beaucoup de livres le disent aussi un poète, auteur de nombreux et célèbres quatrains, mais aucun document ancien ne permet d'identifier le poète et le mathématicien selon Roshdi Rashed. Faut-il être prudent ? Je cite tout de même un vers lu au hasard ou presque, du poète qui aimait le vin, l'amour :

Qui t'amène vive comme le vent pour attiser le feu déjà ardent en ton absence.

Omar Khayyam vit dans une époque troublée. Le calife n'assure plus la protection des savants. Les turcs seldjoukides se sont convertis à l'Islam sunnite et se heurtent aux chiites d'Iran et d'Irak (les tensions entre les deux

7. Al Khwarizmi, *Le calcul indien*, trad. par André Allard, Blanchard, 1992.

communautés ne datent pas d'hier), prennent Bagdad en 1055. En 1070, Omar Khayyam va vivre à Samarcande, sous la protection de l'administrateur de la ville, Abou Tahir. Il est invité à Ispahan, la nouvelle capitale de l'empire turc, par Malik Shah (1055-1092, sultan à partir de 1072) pour s'occuper de l'observatoire de la ville. Après la mort de Malik Shah , il doit attendre 1118 pour retrouver les faveurs d'un sultan, Sanjar, le troisième fils de Malik Shah.

La liste des mathématiciens cités par Omar Khayyam montre une culture étendue. Son traité d'algèbre (écrit vers 1074) est connu par 10 manuscrits, aucun n'étant l'original [8].

Au début du traité, Omar Khayyam donne une esquisse des conditions difficiles de la recherche scientifique à son époque : *Je n'ai pu cependant me consacrer exclusivement à la quête de ce bien, ni y penser avec persévérance, détourné que j'en étais par les vicissitudes du temps. Car nous avons été éprouvés par le dépérissement des hommes de science, à l'exception d'un groupe en nombre aussi petit que ses afflictions sont grandes, et dont le souci est de saisir le temps au vol pour se consacrer cependant à l'achèvement et au perfectionnement de la science. Or, la plupart de ceux de notre temps qui font les savants, déguisent le vrai en faux, ne dépassent jamais les limites de l'imposture et de l'ostentation savante, et n'emploient la quantité de science qu'ils possèdent qu'à des fins corporelles et viles. Et s'ils rencontrent un homme qui s'efforce de rechercher la vérité et privilégie la sincérité, ardent à refuser la fausseté et le mensonge, et à repousser l'ostentation et la tromperie, ils le prennent pour un sot et le tournent en dérision.*

Omar Khayyam est conscient du problème des dimensions créé par l'interprétation des nombres comme segments, des produits de deux nombres comme rectangles, etc. Il l'évoque à plusieurs reprises et propose la solution qui sera reprise par Bombelli et Descartes : *Et si l'algébriste emploie le carré-carré dans les problèmes de géométrie, c'est métaphoriquement, et non pas proprement, étant donné qu'il est impossible que le carré-carré fasse partie des grandeurs. Ce qui se trouve dans les grandeurs, c'est d'abord une seule dimension, c'est-à-dire la seule racine, ou, rapporté à son carré, le côté. Puis les deux dimensions, c'est-à-dire la surface... enfin les trois dimensions, c'est-à-dire le corps... comme il n'existe aucune autre dimension, ne font partie des grandeurs ni le carré-carré ni, à plus forte raison, ce qui lui est supérieur.*

8. Le texte a été publié avec une analyse critique : Rashed Roshdi, *Al Khayyam mathématicien*, Blanchard, 1999.

Et toutes les fois que dans ce traité nous disons : un nombre est égal à une surface, nous entendons par le nombre un quadrilatère à angles droits, dont l'un des deux côtés est un et l'autre une droite égale en mesure au nombre donné... Et toutes les fois que nous disons : un nombre est égal à un solide, nous entendons par nombre un parallélépipède rectangle, dont la base est le carré de l'unité et dont la hauteur est égale au nombre donné.

Le sujet du traité d'algèbre est l'étude détaillée des équations du troisième degré. Omar Khayyam cite Al Khazin (vers 900-971) qui aurait résolu cette équation avec des sections coniques. Ne considérant que des coefficients strictement positifs, Omar Khayyam distingue 25 cas dont 11 se ramènent à des équations de degré inférieur (équations de degré inférieur ou égal à 2 et équations sans termes constants).

Il reste 14 cas où Omar Khayyam obtient les solutions par intersection de coniques : cercles (C), paraboles (P) ou hyperboles (H).

cas	équation	racines	courbes
1	$x^3 = c$	1	PP
2	$x^3 + bx = c$	1	CP
3	$x^3 + c = bx$	0 ou 2	PH
4	$x^3 = bx + c$	1	PH
5	$x^3 + ax^2 = c$	1	PH
6	$x^3 + c = ax^2$	2	PH
7	$x^3 = ax^2 + c$	1	PH
8	$x^3 + ax^2 + bx = c$	1	CH
9	$x^3 + ax^2 + c = bx$	0 ou 2	HH
10	$x^3 + bx + c = ax^2$	0 ou 2	CH
11	$x^3 = ax^2 + bx + c$	1	HH
12	$x^3 + ax^2 = bx + c$	1	HH
13	$x^3 + bx = ax^2 + c$	1 ou 3	CH
14	$x^3 + c = ax^2 + bx$	0 ou 2	HH

Le commentaire complet du texte d'Omar Khayyam est très long et on se reportera à l'édition de Roshdi Rashed. Pour chaque cas, Omar Khayyam donne une construction géométrique et analyse soigneusement les différents cas et les impossibilités. Il ne donne pas systématiquement d'exemple numérique et son traitement est vraiment algébrique, sans le formalisme que nous connaissons maintenant, bien sûr. Les coniques utilisées par Omar Khayyam sont variées,

alors que l'équation $x^3 + ax^2 + bx + c = 0$ s'écrit encore $x^2 + ax = -b - c/x$, qui se résout par une intersection de parabole et d'hyperbole.

Pour $x^3 + ax = b$, Omar Khayyam obtient la solution comme longueur d'un segment construit à l'aide de l'intersection (distincte de 0) de la parabole $y = x^2/\sqrt{a}$ et du cercle $x(x - \frac{b}{a}) + y^2 = 0$.

Pour $x^3 + b = ax$, Omar Khayyam obtient la solution comme longueur d'un segment construit à l'aide de l'intersection de la parabole $y = x^2/\sqrt{a}$ et de l'hyperbole $y^2 = x(x - \frac{b}{a})$.

Pour $x^3 + ax^2 + bx = c$, Omar Khayyam obtient la solution comme longueur d'un segment construit à l'aide de l'intersection du cercle $(x + a)(x - \frac{c}{b}) + (y - \sqrt{b})^2 = 0$ et de l'hyperbole $xy = c/\sqrt{b}$.

Dans ces trois cas, Omar Khayyam remarque qu'il existe toujours une solution (positive) et une seule.

Dans le cas 13, il ne voit pas la possibilité de l'existence de trois racines positives (c'est le cas, par exemple, de l'équation $(x - 1)(x - 2)(x - 3) = 0$).

Dans le cas d'un racine double, Omar Khayyam ne compte qu'une racine.

La justification de l'existence des solutions est donnée : une branche de conique coupe une autre branche de conique quand elle passe de l'autre côté.

Pour la solution algébrique des équations du troisième degré, Omar Khayyam est merveilleusement laconique : *Elle n'est possible ni pour nous, ni pour aucun de ceux qui sont passés maîtres en cette science. Peut-être qu'un de ceux qui viendront après nous la réalisera.* C'est ce qu'écrira aussi Luca Pacioli (1445-1517) en 1494 mais les temps changeaient...[9]

10.4 Travaux sur le cinquième postulat

De nombreux mathématiciens au cours des siècles ont tenté de démontrer le cinquième postulat d'Euclide. Ils arrivaient souvent à produire une démonstration, mais en admettant sans s'en apercevoir une forme équivalente du cinquième postulat, comme : l'ensemble des points équidistants d'une droite et d'un même côté est une droite. Sans avoir de modèle de géométrie non euclidienne (ils datent des années 1860-1880), l'erreur est purement logique et difficile à apercevoir, d'autant plus que le système d'axiomes donné par Euclide est incomplet.

9. La suite de l'histoire est plus loin, voir la section : *L'équation du troisième degré.*

On ne peut parler de tous les travaux arabes sur le cinquième postulat. Parlons seulement de celui d'Abu Ali al Hassan Ibn al Haytham (Khali Jaouiche indique al Hassan ibn al Hassan Ibn al Haytham)(vers 965-1041), connu en Occident sous le nom d'Alhazen, forme latine de son second prénom. Al Haytham serait né à Bassorah comme l'indique la mention d'al Basri. Il a beaucoup écrit, mais la plupart de ses textes sont aujourd'hui perdus. Ses textes les plus connus portent sur l'optique : il explique que la lumière se reflète sur les objets et pénètre dans l'œil, alors que Ptolémée pensait que c'était l'œil qui envoyait de la lumière sur les objets ; il dissèque des yeux ; il pose le problème de déterminer le point de réflexion d'un rayon lumineux sur un miroir sphérique ; il invente la chambre noire (la *camera oscura*), mais j'ai trouvé cette invention attribuée à plusieurs personnes différentes et il faudrait savoir ce qui revient à chacun. Il a des idées sur l'attraction réciproque de deux corps en fonction de leur masse. Il cherche à montrer que les nombres parfaits sont tous de la forme $2^{n-1}(2^n - 1)$ avec $2^n - 1$ premier ; il connaît le théorème de Wilson : $(p-1)! = -1 \bmod p$; il donne un cas particulier du théorème en cherchant les nombres divisibles par 7 et dont la division par 2, 3, 4, 5, 6 donne 1 pour reste.

En géométrie, al Haytham a écrit deux livres de commentaires aux Éléments d'Euclide :

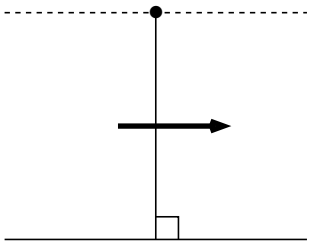
1) Livre expliquant les postulats d'Euclide dans les Éléments ;

2) Livre sur la résolution de ce qui est douteux dans le livre des Éléments d'Euclide (sûrement postérieur au premier, car il s'y réfère).

À l'époque d'al Haytham, plusieurs auteurs ont déjà cherché à montrer le cinquième postulat. Le prolongement des droites à l'infini pose problème depuis au moins Aristote. Comment prolonger indéfiniment des droites limitées dans un univers supposé sphérique et limité par la sphère des fixes ? Al Haytham affirme l'existence des objets mathématiques comme les lignes, les surfaces et les solides dans le domaine des idées, en faisant abstraction des objets concrets : *ceux qui existent pour les sens n'existent pas en vérité car les sens trompent souvent sans que l'opérateur le décèle* alors que *ceux qui existent en imagination existent vraiment et absolument, car la forme qui se façonne elle-même dans l'imagination est réelle puisqu'elle ne disparaît ni ne change.*

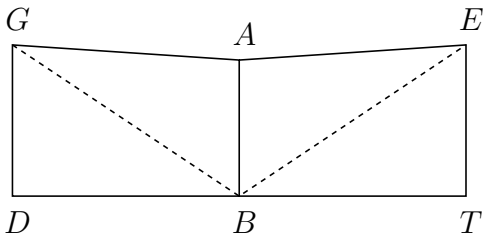
Il faut donc imaginer le prolongement indéfini d'une droite, ce qu'al Haytham propose de faire en mettant bout à bout des segments faisant entre eux un angle plat. La droite ainsi construite peut croître autant qu'on le souhaite par un procédé fini qu'on peut imaginer.

Pour construire une droite parallèle à une autre, Al Haytham utilise le mouvement (uniforme pour lui) ; il considère un segment qui reste dans un plan contenant la droite, dont l'une des extrémités décrit la droite et qui reste perpendiculaire à celle-ci ; l'autre extrémité, affirme al Haytham, décrit alors une droite parallèle.



Du point de vue de la rigueur mathématique, l'erreur est déjà faite ! Omar Khayyam soulignera la faute d'al Haytham.

Suivons maintenant al Haytham dans la démonstration du cinquième postulat. Il commence par construire par un lemme qui sera la base de sa démonstration et le point de départ de tentatives futures. On construit une figure formée d'un segment AB, d'un segment AG perpendiculaires à AB, de la perpendiculaire en B à AB. On projette G sur cette dernière droite en D ; on veut montrer que $GD = AB$. On suppose que ce n'est pas le cas et que $GD > AB$. On prolonge (GA) et on place E tel que $AE = AG$ et on projette E sur (BD) en T.

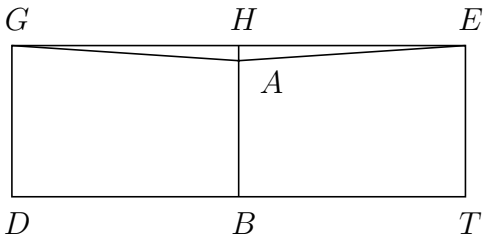


Les démonstrations d'al Haytham sont très détaillées ; nous n'en donnons que l'essentiel (l'essentiel pour moi ; on peut les trouver dans le livre de Khalil Jaouiche).

Al Haytham vérifie d'abord que les triangles rectangles GAB et EAB

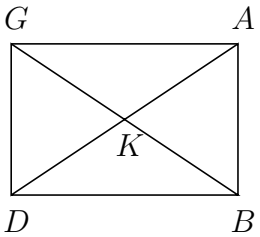
sont égaux ; on en déduit $GB = EB$ et $\widehat{GBA} = \widehat{EBA}$. Par conséquent les complémentaires des deux angles sont égaux ; on a donc l'égalité des triangles GDB et EBT, puis $GD = ET$.

On fait alors bouger le segment ET avec T sur la droite BD en gardant la perpendicularité. Le point E décrit la parallèle à (BD) en passant par G d'après les préliminaires ; quand T est en B, E est en H avec $BH > BA$.



Les droites (EHG) et (EAG) entourent une surface, ce qui est impossible. On montre de même que $GD < AB$ est impossible. Par conséquent $GD = AB$.

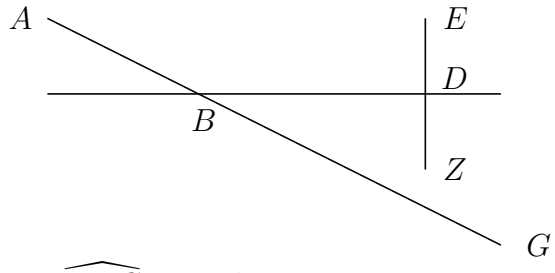
On montre alors que $\widehat{DGA}$ est droit.



L'égalité des triangles GDB et ADB montre les égalités $\widehat{DAB} = \widehat{BGD}$ et $\widehat{BDA} = \widehat{DBG}$. Alors $\widehat{ABK} = \widehat{GDK}$, comme complémentaires des précédents, d'où l'égalité des triangles KDG et KBA, puis $AK = KG$. Dans le tringle isocèle KAG, les angles de base sont égaux. L'angle $\widehat{DGA}$ somme de deux angles égaux à des angles dont la somme est un droit est donc lui-même droit. Ainsi un quadrilatère avec trois angles droits est-il un rectangle.

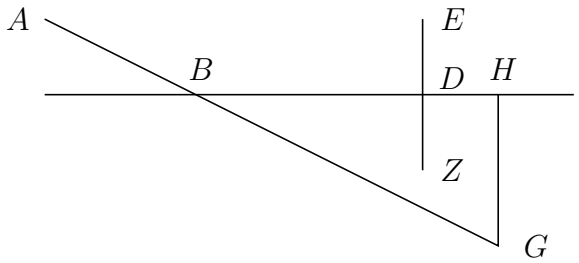
Al Haytham passe alors à la démonstration du cinquième postulat.

Il considère deux droites (AG) et (EZ) coupées en B et D par une droite et suppose que $\widehat{DBG} + \widehat{BDZ} < 2$ dr.

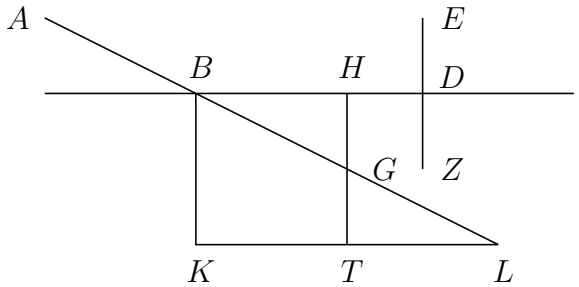


Al Haytham suppose $\widehat{DBG} < 1$ dr ; trois cas peuvent alors se produire : $\widehat{BDZ} <, =, > 1$ dr.

Al Haytham se place d'abord dans le cas $\widehat{BDZ} = 1$ dr., choisit G et le projette sur (BD) en H. Le point H peut être en D et il n'y a plus rien à montrer, au delà de D ou sur le segment BD. S'il est au delà de D, la droite (EZ) entre dans le triangle BHG et ne peut que couper le segment BG ; dans ce cas, le postulat est démontré.



Reste le cas où H est entre B et D. On construit L sur la droite (AB) tel que $GL = GB$ et on place T sur (GH) tel que $GT = GH$. L'égalité des triangles BHG etLTG montre que l'angle $\widehat{GTL}$ est droit. On projette alors T en K sur la perpendiculaire en B à (BD). Le lemme montre que la quadrilatère $BHTK$ est un rectangle. Par conséquent, KTL sont alignés.

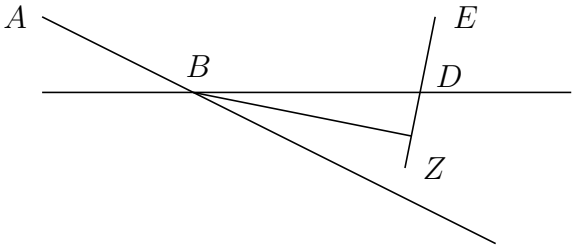


On voit que LK est le double de BH. Si $LK > BD$, on revient au cas précédent ; sinon, on recommence jusqu'à ce que cela ait lieu, en invoquant l'axiome d'Archimède (*clair et à l'abri de toute critique* dit al Haytham, en

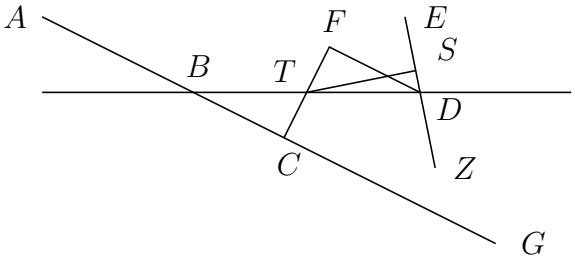
notant qu'Euclide ne l'a pas formulé explicitement).

Le postulat est donc montré dans le cas où (EZ) est perpendiculaire à (BD). Il reste à se ramener à ce cas quand l'angle $\widehat{BDZ}$ n'est pas droit.

On suppose d'abord $\widehat{BDZ}$ aigu. On mène de A la perpendiculaire à (EZ) et on est ramené au cas précédent.



On suppose enfin $\widehat{BDZ}$ obtus. L'angle $\widehat{BDE}$ est alors aigu et supérieur à $\widehat{DBG}$. On prend T milieu de BD et on projette T sur (EZ) en S qui est du côté de E. On trace (DF) avec $\widehat{DBG} = \widehat{BDF}$; (DF) est à l'intérieur de l'angle $\widehat{BDE}$. On note N l'intersection de TS et DF F la projection de T sur DN ; N est entre D et F. D'autre part, on projette T en C sur (BG). Les triangles TCB et TDF sont égaux, ce qui montre que C, T, F sont alignés.



On voit alors que CS forme deux angles aigus avec les deux droites (AG) et (EZ). Ces droites ce coupent donc d'après ce qu'on a déjà vu. Al Haytham croit donc avoir montré le cinquième postulat.