INSTITUT
DE RECHERCHE
POUR L'ENSEIGNEMENT
DES MATHEMATIQUES

n°17

JUIN 2002

M. : A. T. H.

MNEMOSYNE

UNIVERSITE DENIS DIDEROT
PARIS VII

Cette brochure est réalisée par l'IREM PARIS 7 DENIS DIDEROT avec le concours de la D.L.C., des MAFPEN de Paris, Créteil et Versailles et de Nadine LOCUFIER à la reprographie.

Mnémosyne

personnification de la mémoire.

Elle s'unit à Zeus pendant 9 nuits de suite ;

de cette union naquirent les neufs Muses.

(Dictionnaire Robert des noms propres)

Illustration de la couverture : « **La mémoire** »

gravure allégorique d'après Gravelot (XVII[e] siècle)

MNEMOSYNE

M: *Mathématiques*

A. *Approche par les*

T. *textes*

H. *historiques*

Marin Mersenne
de L'ordre des peres Minimes

SOMMAIRE

Editorial — *Jean-Luc Verley* — *p.5*

Bonnes vieilles pages — *Eugène Carissan* — *p.7*
Machine à résoudre les congruences

Etude — *p.17*
Factorisation de grands nombres : de Fermat à la machine des frères Carissan.
Martine Bühler

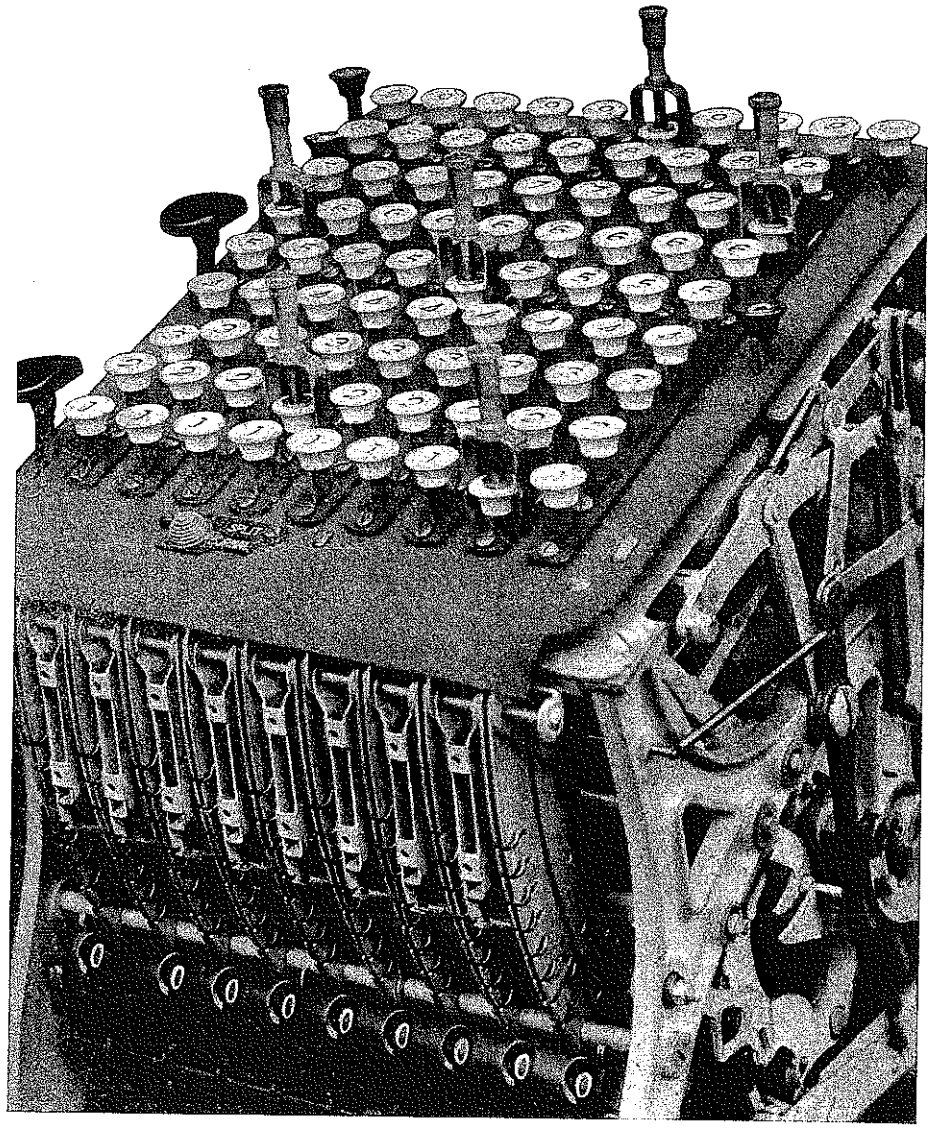
Conte du Lundi I — *p.31*
Arithmétique et codes secrets. Un coup d'œil historique.
Martine Bühler

Mathématiques et théâtre — *p.49*
Breaking the code *Hugh Whitemore*
Anne Michel-Pajus

Dans nos classes — *p.53*
Méthode de Fermat par factoriser les grands nombres.
Martine Bühler

Notes de lecture — *Anne Michel-Pajus* — *p.59*

Conte du Lundi II — *Rudolf Bkouche* — *p.61*



MACHINE à CONGRUENCES

André GÉRARDIN

(MODÈLE 1937)

Electrique, Imprimante, Automatique

EDITORIAL

L'essentiel de ce *Mnémosyne* 17 est constitué par deux articles de Martine Bühler où la théorie des nombres, la "reine des mathématiques ", joue un rôle dominant, dans un cadre peu habituel. Comme souvent dans ce domaine, on trouve à l'origine une préoccupation de FERMAT. La décomposition des grands nombres en facteurs est très difficile sur le plan pratique ; bien qu'il y ait de nombreuses méthodes, aucune ne marche à coup sûr. Au début du XX^{e} siècle, les frères Pierre et Eugène CARISSAN ont inventé et réalisé une curieuse machine à factoriser dont le principe utilise la théorie des congruences arithmétiques. Après une véritable enquête policière (le minitel s'est avéré un outil fantastique), une équipe américaine a découvert, à l'observatoire de Floirac, près de Bordeaux, l'unique exemplaire actuellement connu de cette machine ; il a été transféré au C.N.A.M. en 1994 où il est maintenant à la disposition des chercheurs.

Le deuxième article de ce numéro de *Mnémosyne* peut donner un exemple de réponse à cette interrogation de nos élèves : "à quoi çà sert ? ".

Le souci de communiquer à l'abri des yeux et des oreilles indiscrets est aussi ancien que l'Humanité (il me plaît d'imaginer que les amoureux ont précédé les militaires...). C'est en tout cas en vue d'applications diplomatico-militaires que fut développée la cryptographie. Les mathématiques y sont omniprésentes, y compris dans le vocabulaire : le service correspondant s'appelle encore de nos jours le "service du chiffre". Et nous retrouvons, trois siècles plus tard, les recherches de Fermat dans un des procédés les plus récents de cryptographie : la sécurité du système R.S.A. repose sur la difficulté de factoriser rapidement de très grands nombres.

La cryptographie fascine petits ou grands (le "ou" est la disjonction logique, non exclusive), mais attention ! Si elle peut conduire à la gloire (pendant la guerre avec l'Espagne, Viète déchiffra le codage espagnol et fut nommé conseiller d'Henri IV ; Alan Turing fut ennobli), elle peut aussi, si elle devient une obsession, conduire à la folie. Terminons donc sur une note d'actualité, en faisant allusion au film de Ron Howard, *Un homme d'exception* (*A beautiful mind*, 2001), sorti récemment sur nos écrans ; c'est une biographie romancée du mathématicien John Nash, né en 1928, prix Nobel d'Economie en 1994 pour ses travaux de jeunesse. Spécialiste du chiffre pour les militaires américains pendant la seconde guerre mondiale, il se crut (ou fut ?) persécuté par les services secrets et développa à l'âge de trente ans une forme aigue de schizophrénie. S'il a depuis quelques années repris ses recherches, il a passé de longues années en hôpital psychiatrique, avec de courtes périodes de répit.

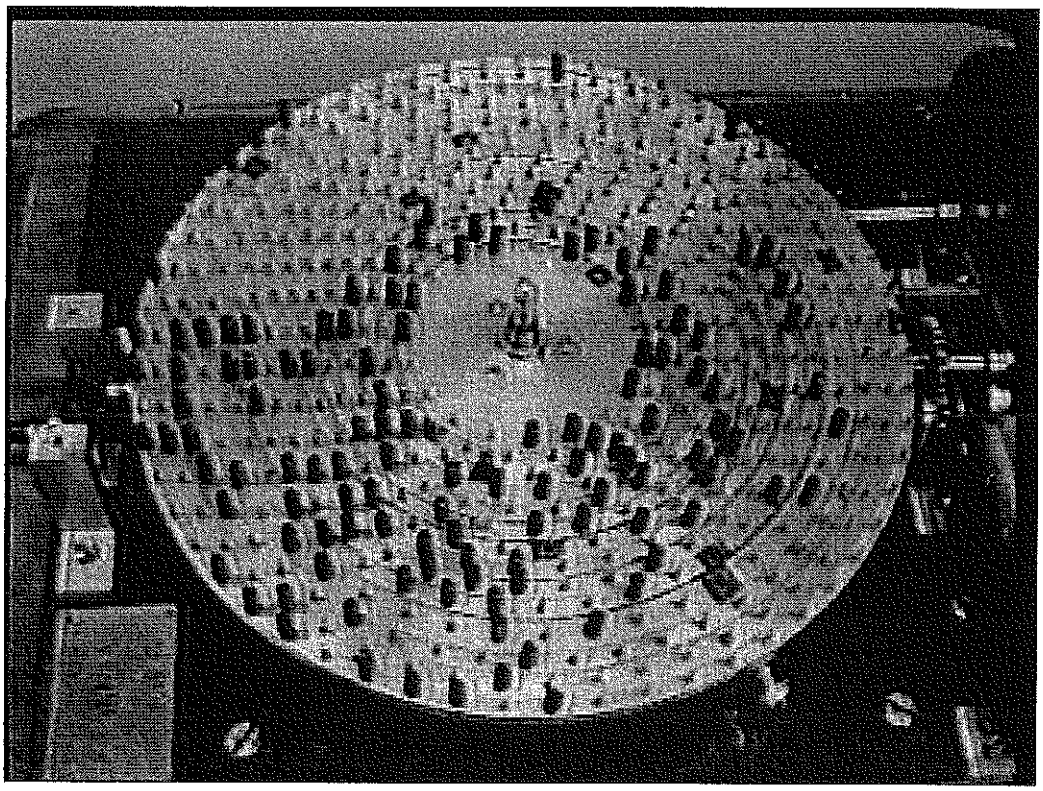
Jean-Luc Verley


PIERRE DE FERMAT 1601 · 1665
RF
LA POSTE 2001
4,50 F
0,69 €
$x^n + y^n = z^n$
n'a pas de solution pour des entiers $n \geq 2$
LAVERGNE

PIERRE DE FERMAT 1601-1665
1er jour 18.08.2001
82 BEAUMONT DE LOMAGNE

BONNES VIEILLES PAGES

Nous présentons ici le texte intégral de l'article d' Eugène Carissan paru en 1920 dans le *Bulletin de la Société d'Encouragement à l'Industrie Nationale*, article dans lequel il explique le fonctionnement de sa machine à congruences[1]. Ci-dessous, une photographie de la machine de Carissan, prise au Musée des Arts et Métiers.



[1] Pour plus de précisions, voir l'étude page 15 de ce numéro.

MACHINE A RÉSOUDRE LES CONGRUENCES[1]

But. — Cet appareil, qui a figuré à l'Exposition de machines à calculer organisée par la Société d'Encouragement du 5 au 13 juin 1920, a pour but la résolution mécanique, en nombres entiers, des équations indéterminées à deux variables.

Principe. — La machine est une application de la théorie des congruences, et des méthodes d'utilisation de cette théorie qu'a instituées M. André Gérardin, de Nancy (2), pour la résolution des équations indéterminées.

Soit, à titre d'exemple simple, à résoudre en nombres entiers l'équation :

$$x^2 - 6y^2 = 1\,324\,801 = A$$

ou

$$6y^2 + A = x^2. \qquad (1)$$

On envisage successivement les diverses hypothèses possibles : $y =$ mult. de $m + 0, 1, 2, \ldots (m - 1)$, pour un certain nombre de diviseurs ou modules m, et on examine dans chacune de ces hypothèses s'il y a compatibilité entre le premier et le deuxième membre de l'équation (1), en tenant compte de ce fait que x^2 ne peut avoir, pour un module déterminé, que certaines valeurs connues à l'avance (résidus quadratiques).

Soit à appliquer le module 5; on a, en remarquant que A est un mult. de $5 + 1$, et que les résidus quadratiques (valeurs de x^2) ne peuvent être, en module 5, que 0, 1, 4 :

1re hypothèse :
$y =$ mult. de $5 + 0$; $6y^2 =$ mult. de $5 + 0$; $6y^2 + A =$ mult. $5 + 1 \ldots$ combinaison *possible*.
2e et 5e hypothèses :
$y =$ mult. de 5 ± 1; $6y^2 =$ mult. de $5 + 1$; $6y^2 + A =$ mult. $5 + 2 \ldots$ — *impossible*.
3e et 4e hypothèses :
$y =$ mult. de 5 ± 2; $6y^2 =$ mult. de $5 + 4$; $6y^2 + A =$ mult. $5 + 0 \ldots$ — *possible*.

En résumé, y ne peut être que mult. de $5 + 0$; mult. de $5 + 2$; mult. de $5 + 3$, ce que nous exprimons par la *bande modulaire* 0I00I, dans laquelle : le signe 0 marque la possibilité, le signe I l'impossibilité.

(1) Communication faite en séance publique par l'auteur le 26 juin 1920.
(2) Directeur de la revue : *Le Sphinx-Œdipe*, 32, Quai Claude-Le-Lorrain, Nancy.

De même, appliquons le module 7 (en remarquant que A est un mult. de $7+2$, et que x^2, en module 7, ne peut être égal qu'à 0, 1, 2, 4) :

1re hypothèse :
y = mult. de $7+0$; $6y^2$ = mult. de $7+0$; $6y^2+A$ = mult. $7+2$ ... combinaison *possible*.
2e et 7e hypothèses :
y = mult. de 7 ± 1 ; $6y^2$ = mult. de $7+6$; $6y^2+A$ = mult. $7+1$ ... — *possible*.
3e et 6e hypothèses :
y = mult. de 7 ± 2 ; $6y^2$ = mult. de $7+3$; $6y^2+A$ = mult. $7+5$ ... — *impossible*.
4e et 5e hypothèses :
y = mult. de 7 ± 3 ; $6y^2$ = mult. de $7+5$; $6y^2+A$ = mult. $7+0$ ... — *possible*.

Bande modulaire correspondante : 00I00I0.

En opérant pareillement avec d'autres modules, 11, 13, 17..., on obtiendrait d'autres bandes modulaires, comportant également d'autres conditions pour y. Or, un nombre quelconque est un multiple du module $m+0, 1, 2, 3, \ldots (m-1)$, c'est-à-dire correspond à l'une des cases de la bande modulaire en m. Il sera *solution* si les cases auxquelles il correspond sur les bandes des différents modules comportent, toutes à la fois, le signe de possibilité.

Le rôle d'une *machine* propre à rechercher cette solution sera donc de juxtaposer toutes les bandes modulaires établies, en faisant correspondre les cases de même rang, et d'avertir l'opérateur lorsqu'à un rang déterminé, toutes les bandes comporteront le signe de possibilité. Pour ce faire, la machine doit renouveler automatiquement la bande de chaque module, dès qu'elle a été utilisée.

Le tableau suivant montre la disposition des bandes juxtaposées, au moment où apparaît la première solution de l'équation (1) autre que 0.

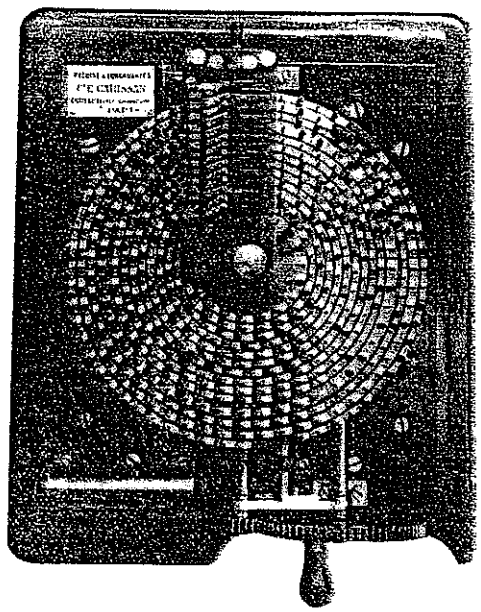
Série naturelle des nombres .	135	136	137	138	139	140	141	142	143	144
Module 5.	0	I	0	0	I	$\underline{0}$	I	0	0	I
— 7.	I	0	0	I	0	$\underline{0}$	0	I	0	0
— 11.	0	I	0	0	I	$\underline{0}$	I	0	0	0
— 13.	0	I	I	0	I	$\underline{0}$	I	0	0	0
— 17.	I	0	I	0	I	$\underline{0}$	I	I	0	0
— 19.	I	0	I	0	I	$\underline{0}$	0	I	I	0
. . . . .										

c'est-à-dire $y = 140$, correspondant à $x = 1\,201$.

Historique. — Indépendamment des machines personnelles de M. Gérardin, et de celle envisagée par M. Kraïtchik, un premier modèle de machine basée sur le principe théorique ci-dessus fut conçu en 1912 par M. P. Carissan, professeur au collège de Lesneven; ce modèle, construit par le lieutenant

E. Carissan, et présenté au Congrès de Nîmes de l'Association française pour l'Avancement des Sciences, en 1912, par M. Gérardin, utilisait des bandes modulaires fermées, souples, pendantes, entraînées simultanément par un même cylindre cannelé, avec décel optique des solutions : mais le rendement était faible.

En 1913-1914, le lieutenant Carissan conçoit et construit de ses mains un premier modèle de la machine à congruences actuelle : les résultats sont si encourageants, qu'ils paraissent justifier les frais d'une construction de précision, laquelle fut confiée à la Maison Château Frères, de Paris. La guerre interrompit cette construction, et l'appareil définitif du commandant E. Carissan ne put être achevé qu'à la fin de 1919.



I. — L'appareil monté vu en plan.

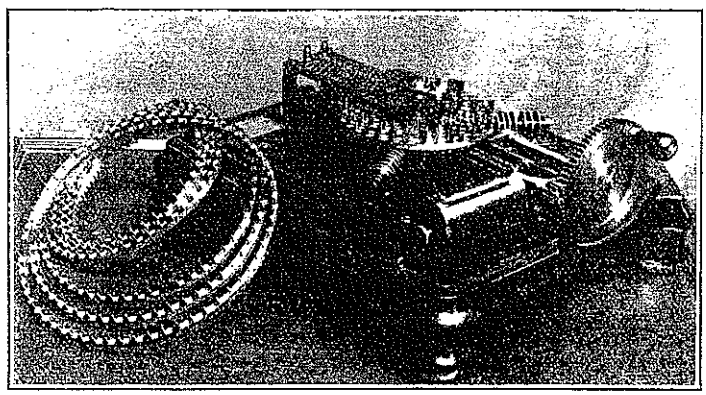
Description de la machine du commandant E. Carissan (fig. I et II). — Des couronnes métalliques concentriques, figurant les bandes modulaires, sont soutenues dans le même plan horizontal par trois lignes de galets à 120°. Elles sont dentées sur leur face inférieure : les dentures, toutes de même pas, sont taillées de manière que les couronnes puissent être toutes entraînées simultanément (mais non avec la même vitesse) par un même long pignon dont l'axe est parallèle au plan des couronnes, et passe par leur axe de rotation commun.

Chaque couronne porte, vissées normalement sur sa face supérieure, des broches d'acier *équidistantes*. Les nombres de ces broches, portées par les différentes couronnes, sont les nombres premiers jusqu'à 59 (modules). Les dents inférieures de chaque couronne sont en nombre *double*. De la sorte, il est possible, en choisissant les dents des couronnes mises en prise avec le pignon entraîneur, de réaliser *l'alignement des broches suivant un rayon*, prolongement de celui suivant lequel les couronnes sont en prise.

Lorsque le pignon entraîneur tourne sur son axe, les couronnes tournent concentriquement toutes à la fois *du même nombre de dents*, et l'alignement radial des broches se renouvelle, au moment où elles passent sur le rayon fixe, dit *ligne d'investigation*.

Chaque couronne figurant une bande modulaire, les *possibilités* sont représentées par de petites *coiffes* de fibre, enfilées sur les broches voulues. Les alignements des broches se succédant par la rotation des couronnes sont donc composées de broches garnies et non garnies de coiffes. Lorsque un alignement ne comporte que des coiffes, il y a *solution*.

Décel automatique des solutions. — La machine avertit lorsqu'un tel alignement passe sur la ligne d'investigation. L'organe préposé à ce décel ou *herse* est composé d'une série de petits marteaux de cuivre, de forme demi-cylindrique, portés par des ressorts légers, montés sur une plaquette de fibre,



II. — Vue perspective de l'appareil (des couronnes modulaires ont été retirées pour montrer le dispositif d'entraînement).

au-dessus des passages respectifs des broches des différentes couronnes. A chaque marteau correspond une coupure d'un circuit électrique sur lequel sont montés en série une pile sèche et un récepteur téléphonique.

Lorsqu'une coiffe passe sous la herse, comme sa hauteur est un peu plus grande que celle de la broche qui lui sert de support, le marteau correspondant est soulevé, et sa coupure annulée. Quand tous les marteaux sont soulevés à la fois, toutes les coupures, qui sont en série, sont annulées à la fois, et le courant passe. L'opérateur est averti par un *toc* caractéristique du téléphone.

Détails du mécanisme. — Couronnes. — Afin de réduire à la fois le frottement mutuel des couronnes et leurs déplacements latéraux, chacune d'elles est pourvue, sur sa face inférieure, et à côté de la denture, d'un chemin de roulement pour les galets qui lui servent de support.

Les broches de chaque couronne sont numérotées $1, 2, 3, \ldots m$. L'origine (m) de chaque couronne est peinte en rouge; sa moitié marquée d'un repère noir.

Afin d'obtenir un encombrement minimum, et plus d'uniformité dans la largeur des couronnes modulaires (largeur qui est commandée par le nombre des côtés du polygone régulier, *de côté constant*, à y inscrire), les différentes couronnes représentent — du centre à la périphérie — les modules :

19, 3×7, 23, 2×13, 29, 31, 2×17, 37, 41, 43, 47, 53, 5×11, 59,

c'est-à-dire 17 modules répartis sur 14 couronnes, les bandes correspondant aux modules composés (2×13, 2×17, 3×7, 5×11) étant obtenues par la combinaison des modules simples.

Embrayage et débrayage. — Une manette extérieure permet d'embrayer ou de désembrayer simultanément toutes les couronnes, par effacement du pignon entraîneur. Ce dispositif permet : de rendre folles les couronnes, ce qui rend plus aisé le placement préalable des coiffes; le cas échéant, de placer, avant de mettre la machine en marche, chaque couronne dans la position qu'elle occuperait si l'appareil avait déjà fonctionné jusqu'à une valeur donnée. En un mot, ce dispositif permet de commencer l'investigation à partir d'un nombre arbitraire, si grand soit-il, en s'épargnant une révolution dont l'inutilité aurait été reconnue *a priori*.

Compteur. — Un compteur, allant jusqu'à 10^6, et commandé par le pignon d'entraînement, donne à chaque instant le rang de la ligne de broches passant sur la ligne d'investigation. Il est à apparition brusque des chiffres, et comporte un organe de débrayage et de remise au zéro.

Commande de la machine. — Elle se fait à la main, par l'intermédiaire d'un volant denté multiplicateur. Un dispositif de commande par moteur électrique, avec rupture automatique du circuit du moteur, et arrêt (par l'intermédiaire d'un relai) du fait même du passage d'une solution, est à l'étude.

Récepteur téléphonique. — Pour plus de commodité, le récepteur téléphonique est remplacé par un *casque* téléphonique; dans ces conditions, la netteté du signal acoustique est telle que l'opérateur n'a nul besoin de concentrer son attention pour être à coup sûr averti, quelle que soit la rapidité de rotation de la machine.

Disposition d'ensemble. — L'ensemble de la machine est porté par un socle en ébénisterie, reposant sur cales de caoutchouc. Un couvercle en tôle laquée, qui s'emboîte sur la platine de l'appareil, protège ses organes contre la poussière.

Utilisation de la machine. — Les bandes modulaires étant établies pour l'équation à résoudre, débrayer la machine, placer les coiffes sur les broches

voulues de chaque couronne, en s'aidant du numérotage. Deux cas peuvent alors se présenter :

1° *L'investigation doit commencer à partir de zéro* : placer les repères rouges sous la herse, ce qui amène les repères noirs à former une ligne continue (au-dessus de la ligne d'entraînement par le pignon);

2° *L'investigation doit commencer à partir d'un nombre* N : dans ce cas, déterminer d'abord les restes (résidus) de la division de N par les modules qu'utilise la machine (19, 21, 23... 59), et placer chaque couronne de manière que le nombre, résidu correspondant à son module, soit sur la ligne d'investigation.

Dans les deux cas, les couronnes une fois placées, embrayer. Mettre le compteur au zéro, puis mettre en place le dispositif avertisseur téléphonique, en serrant sous les bornes *ad hoc* les extrémités du circuit pile-casque téléphonique. L'opérateur, muni du casque, n'a plus alors qu'à tourner à vitesse modérée (2 tours à la seconde) le volant d'entraînement. Lorsqu'une solution « passera », ce dont le téléphone avertira, arrêter la rotation sans brutalité, revenir en arrière doucement, en observant les alignements, jusqu'au moment où le toc se reproduit. Lire alors le compteur qui donne la valeur cherchée (ajouter le nombre N s'il y a lieu).

Puissance et rendement de la machine. — Les nombres de broches portées par les différentes couronnes étant premiers entre eux, la machine ne reproduira exactement une même disposition initiale relative des couronnes que quand elle aura examiné un nombre d'unités égal au produit des modules entre eux, qui est un nombre de 22 chiffres. Pratiquement, la *puissance* de la machine peut donc être considérée comme illimitée.

Il est prévu que des nombres satisfaisant à l'ensemble des conditions imposées par les bandes modulaires, et qui sont par conséquent livrés par la machine, peuvent ne pas être solutions de l'équation proposée. (Ces nombres, ou *pseudo-solutions*, auraient été éliminés par la mise en jeu de modules supplémentaires.) Mais étant donné le nombre des couronnes, la probabilité pour qu'un nombre fourni par la machine soit solution réelle est considérable.

Le temps nécessaire pour l'obtention d'une solution est extrêmement variable suivant les équations, depuis quelques secondes jusqu'à plusieurs heures. Des équations n'admettant *aucune* solution entière peuvent être soumises à la machine : celle-ci restera alors indéfiniment muette.

Le *rendement* de la machine est normalement de 35 à 40 nombres examinés *à la seconde*, soit de 2 000 à 2 400 *à la minute*. La rapidité de rotation ne compromet pas la netteté du signal avertisseur, bien que la durée du courant qui produit ce dernier ne soit pas supérieure à $\frac{1}{250}$ de seconde.

Applications de la machine. — La machine permet l'obtention directe des solutions entières des équations à deux variables, de la forme générale :

$$f(x) = \varphi(y).$$

La grandeur et le signe des coefficients et des exposants — pourvu qu'ils soient entiers — sont indifférents.

Son emploi est indiqué pour toutes les équations de cette sorte pour lesquelles l'existence et la valeur des solutions ne pouvant être prévues par la théorie des nombres, la résolution doit être recherchée par la voie expérimentale.

En particulier, l'appareil est appliqué avec succès à la décomposition des grands nombres, la recherche des nombres premiers, et l'étude de leur répartition.

L'intérêt de la machine reste, jusqu'à nouvel ordre, purement spéculatif. Mais il n'est nullement démontré que l'astronomie, par exemple, ne puisse retirer de son emploi un bénéfice positif.

Exemples de questions traitées avec la machine.

Résoudre :

$x^2 - 13y^2 = 1$ (pour $x < 10\,000$)	
$x = 649 ; \quad y = 180.$	(5 minutes)
$2u^2 + v^2 = 708\,158\,977$	
$u = 14\,676 ; \quad v = 16\,655.$	(8 minutes)
$x^2 - 6y^2 = 1\,151^2$ (pour x et $y < 13\,000$)	
$x = 0,\ 1\,201,\ 7\,685 ;\ y = 0,\ 140,\ 3\,102.$	(7 minute)
$x^3 \pm y^3 = 756\,249\,048$	
$x = 919,\ -271 ;\ y = \pm 271,\ \pm 919.$	(8 minutes)

*
* *

Mettre sous la forme de la somme de deux carrés :

$708\,158\,977 = 19\,224^2 + 18\,401^2.$	(10 minutes)
$1\,321\,442\,641 = 25\,704^2 + 25\,705^2.$	(15 minutes)
$18\,405\,321\,661 = 95\,930^2 + 95\,931^2.$	(1 heure)

*
* *

Reconnaître si les nombres suivants sont premiers : le cas échéant, donner leurs facteurs ;

$A = 62\,080\,247$. Réponse affirmative : ne peut être mis que d'une seule façon sous la forme $x^2 - 2y^2$ ($x = 9\,005$, $y = 3\,083$, qui sont premiers entre eux) (3 minutes de rotation).

$A = 225\,058\,681$. Réponse négative : $A = 1\,909^2 + 14\,880^2$ et $A = 5\,741^2 + 13\,860^2$, d'où l'on tire : $A = 229 \times 982\,789$ (5 minutes).

$A = 3\,450\,315\,521$. Réponse négative : $A = 2\,975^2 + 58\,664^2$ et $A = 3\,664^2 + 58\,625^2$, d'où l'on tire : $A = 2\,448\,769 \times 1\,409$ (2 minutes).

$A = 2^{31} - 1 = 2\,147\,483\,647$. Réponse affirmative, en employant successivement deux méthodes (17 minutes et 15 minutes) :

$A = 65\,535^2 - 2 \times 32\,767^2$. Seule décomp. de cette forme, facteurs premiers entre eux.

$A = 4 \times 23\,081^2 + 3 \times 2\,349^2$. Seule décomp. de cette forme, facteurs premiers entre eux.

$A = 3\,570\,537\,526\,921$. Réponse négative. Le point de départ de l'investigation a été 1 336 000, voisin de la racine carrée de A. La machine a donné en 18 minutes les deux décompositions :

$A = 1\,336\,139^2 + 1\,336\,140^2$ et $A = 1\,370\,700^2 + 1\,300\,661^2$, d'où l'on tire : $3\,570\,537\,526\,921 = 841\,249 \times 4\,244\,329$.

COMMANDANT E. CARISSAN.

Vient de paraître

Le Tome 3

de

Mathématiques : Approche par les Textes Historiques

Le groupe M:.A.T.H poursuit la publication de documents pédagogiques utilisant des textes historiques originaux.

Les huit documents proposés dans ce tome s'adressent plutôt à des élèves de lycée. Ils ont tous été expérimentés en classe.

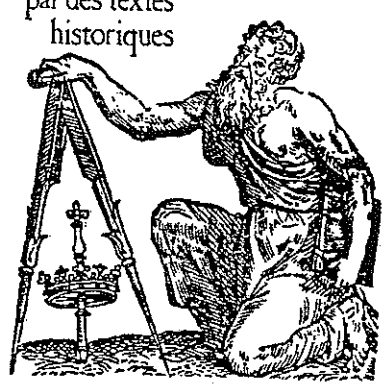
Les outils mathématiques nécessaires aux élèves sont en rapport avec les programmes des lycées et sont indiqués au début de chaque activité.

Vous Y trouverez :

La section dorée	Euclide
Une méthode de résolution d'une équation du 3ème degré	Viète
Les satellites de Jupiter	Galilée
La mesure du méridien	Picard, Delambre, Legendre
Le volume de la pyramide	Legendre
Une approximation de π	Euler
Différences finies et Sommation de séries	Leibniz
Lettre de Leibniz à La Roque	Leibniz

Brochure n°91
Juillet 2001
IREM
Université Paris VII Denis Diderot
175, rue du Chevaleret
Paris 13ème
Tel : 01 44 27 53 83

mathématiques approche par des textes historiques M:A.T.H.



FACTORISATION DE GRANDS NOMBRES : DE FERMAT A LA MACHINE DES FRERES CARISSAN

Martine Bühler

On apprend dès l'école primaire à calculer le produit de deux nombres entiers, même grands, « à la main ». Mais l'opération inverse (factoriser un grand nombre entier) se révèle très ardue. Les mathématiciens se sont intéressés à ce problème, sans doute au départ comme à un défi intellectuel. On trouve ainsi dans les lettres de Fermat des indications à ce sujet.

La correspondance de Fermat

Les formes de l'activité mathématique au XVII^{ème} siècle ne sont pas unifiées. Il y a plusieurs sources de problèmes : traductions des œuvres de mathématiciens grecs (Euclide, Apollonius, Archimède, Diophante,...) ; navigation ; travaux des ingénieurs et artilleurs etc. Les publications mathématiques sont difficiles et assez rares, en particulier à cause de problèmes typographiques d'impression ; il n'y a pas de journaux scientifiques au début du dix-septième : ils feront leur apparition vers 1665, en même temps que l'Académie des Sciences. Fermat n'a jamais écrit de traité de théorie des nombres ; on connaît ses travaux à ce sujet par sa correspondance. A partir de 1636, par l'intermédiaire de Carcavi, son collègue au Parlement de Toulouse, Fermat rencontre le cercle de Mersenne et commence à correspondre avec ce dernier. Mersenne est un personnage essentiel de l'époque[1] ; il échange des lettres sur de multiples sujets philosophiques et scientifiques avec des correspondants de l'Europe entière : Roberval, Pascal, Hobbes, Descartes, Gassendi,... Il a plusieurs centaines de correspondants en Europe et même jusqu'en Turquie. Les lettres sont recopiées, réexpédiées, remaniées. Les mathématiciens s'envoient des problèmes, des solutions, des défis. Les lettres de Fermat que nous allons examiner sont des réponses à un défi de Mersenne.

Lettre de Fermat à Mersenne du mardi 7 avril 1643
Extrait des *Œuvres*, ed. Tannery et Henry, tome II, 1894

4. Vous me demandiez donc quelle proportion a le nombre, qui se produit des nombres suivants,
avec ses parties aliquotes :

214 748 364 800 000, 11, 19, 43, 61, 83, 169, 223, 331, 379, 601, 757, 961,
1 201, 7 019, 823 543, 616 318 177, 6 561, 100 895 598 169.

Vous me demandiez ensuite si ce dernier nombre est premier ou non, et une méthode pour découvrir dans l'espace d'un jour s'il est premier ou composé.

A la première question, je vous réponds que le nombre qui se fait de tous les nombres précédents multipliés entre eux, est sous-quintuple de ses parties.

A la seconde question, je vous réponds que le dernier de ces nombres est composé et se fait du produit de ces deux :

898 423 et 112 303,

qui sont premiers.

Je suis toujours, mon Révérend Père,

[1] Le Père Marin Mersenne (1588-1648) a fait ses études chez les Jésuites au collège de la Flèche puis est entré chez les Minimes.

Votre très humble et très affectionné serviteur,
FERMAT.

A Toulouse, ce 7 avril 1643.

Cette lettre mérite quelques explications. Une partie aliquote d'un entier N est un diviseur de N différent de N. On cherche la proportion d'un nombre N avec ses parties aliquotes, c'est-à-dire avec la somme s(N) de ses diviseurs différents de lui-même (le diviseur 1 étant compris). La réponse de Fermat stipule que s(N) = 5N. Nous donnons dans l'annexe 1 des indications permettant d'obtenir ce résultat. Fermat affirme ensuite que 100 895598169 = 898 423 x 112 303, résultat stupéfiant[2]. Il ne donne cependant pas ici de méthode générale de factorisation mais seulement la réponse. Dans une autre lettre, qu'on imagine postérieure mais sans pouvoir précisément la dater, Fermat propose une méthode. Nous allons étudier cette lettre de près.

Lettre de Fermat à Mersenne (1643)
Extrait des *Œuvres*, ed. Tannery et Henry, tome II, 1894

Tout nombre impair non quarré est différent d'un quarré par un quarré, ou est la différence de deux quarrés, autant de fois qu'il est composé de deux nombres, et, si les quarrés sont premiers entre eux, les nombres compositeurs le sont aussi. Mais si les quarrés ont entre eux un commun diviseur, le nombre en question sera aussi divisible par le même commun diviseur, et les nombres compositeurs seront divisibles par le côté de ce commun diviseur.

Par exemple : 45 est composé de 5 et de 9, de 3 et de 15, de 1 et de 45. Partant, il sera trois fois la différence de deux quarrés : savoir de 4 et de 49, qui sont premiers entre eux, comme aussi sont les compositeurs correspondants 5 et 9 ; plus, de 36 et de 81, qui ont 9 pour commun diviseur, et les compositeurs correspondants, 3 et 15, ont le côté de 9, savoir 3, pour commun diviseur ; enfin 45 est la différence de 484 et 529, qui ont 1 et 45 pour compositeurs correspondants.

Il est fort aisé de trouver les quarrés satisfaisants, quand on a le nombre et ses parties, et d'avoir les parties lorsqu'on a les quarrés.

Pour nous, il s'agit de l'application d'une identité remarquable et on peut faire lire ce texte à des élèves de troisième. Si $N = a^2 - b^2$ avec a et b entiers, alors $N = (a + b) \times (a - b)$ et $N = p.q$ avec $p = a + b$ et $q = a - b$ entiers. Réciproquement si un nombre entier impair N est égal à un produit d'entiers p.q, alors p et q sont tous deux impairs et $N = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$ avec $\left(\frac{p+q}{2}\right)$ et $\left(\frac{p-q}{2}\right)$ entiers. Il est donc équivalent de factoriser un nombre entier impair ou de le mettre sous forme de différence de deux carrés. Ayant à factoriser un grand nombre, par exemple N = 2 027 651 281, on cherche a et b tels que $N = a^2 - b^2$. On cherche donc un nombre entier a tel que $a^2 - N$ est un carré parfait ; on commence les recherches à $a = E(\sqrt{N}) + 1$ car c'est la première valeur de a qui rend a^2 - N positif. Ensuite on essaie a + 1, a + 2, a + 3,...jusqu'à ce que cela marche. La suite du texte, que vous trouverez dans la rubrique *Dans nos classes* page 53,avec un problème bâti à partir du texte, donne un algorithme de calcul[3] qui permet d'éviter les élévations au carré dans la recherche de a et b. Fermat factorise ainsi 2 027 651 281 en douze étapes alors que la méthode « naturelle » par divisions successives aurait nécessité d'essayer tous les nombres premiers jusqu'à 44 021. Dans ce cas, la méthode proposée par Fermat est donc nettement plus efficace que la méthode courante. Quand cela se produit-il exactement ?

[2] Vous pouvez vérifier : c'est juste ! La TI89 donne cette factorisation quand on utilise le programme Factor mais la TI92 reste persuadée que N est premier, tout en calculant correctement le produit des deux facteurs.

[3] L'étude détaillée de cet algorithme est faite dans le devoir donné en terminale S comme aide à la lecture du texte.

Lorsque $N = a^2 - b^2$, le nombre d'étapes de l'algorithme de Fermat est $a - (Ent(\sqrt{N}) + 1)$ c'est-à-dire si on revient aux facteurs p et q de N environ $\frac{p+q}{2} - \sqrt{pq} = \frac{\left(\sqrt{p} - \sqrt{q}\right)^2}{2}$. La méthode est donc particulièrement efficace si les facteurs p et q de N sont « proches ». On peut se demander si Fermat a utilisé sa méthode pour factoriser 100 895 598 169 dans sa réponse au défi de Mersenne ; le nombre d'étapes nécessaires est alors 187 721 et il y a fort à parier qu'il a procédé autrement. Tannery, dans son édition des œuvres de Fermat, donne une indication sur la procédure peut-être employée, développée dans l'annexe 1.

Qu'en est-il si N est premier ? Alors la seule décomposition possible est N = N.1 donc $a = \frac{N+1}{2}$. La méthode permet donc d'affirmer que N est premier si la seule solution trouvée est $a = \frac{N+1}{2}$ mais le nombre d'étapes est alors à peu près $\frac{N+1}{2} - \sqrt{N} = \frac{\left(\sqrt{N} - 1\right)^2}{2}$ et en tant que test de primalité la méthode n'est pas efficace.

Fermat ramène donc le problème de la factorisation d'un grand nombre à celui de savoir si un nombre entier est ou non un carré. Il fait alors une remarque qui aura de l'avenir : il est immédiat que certains nombres **ne sont pas des carrés** car les carrés, en numération décimale, ne se termine pas par n'importe quoi ; par exemple, 49 619 ne peut pas être un carré *parce que aucun carré* ne finit par 19. Ainsi, l'inspection des « finales » permet d'éliminer un grand nombre de valeurs de a car on voit immédiatement que $a^2 - N$ n'est pas un carré. C'est cette remarque que vont généraliser les frères Carissan pour mécaniser l'algorithme de résolution.

La machine des frères Carissan

Pierre et Eugène Carissan sont nés respectivement en 1871 et 1880. Pierre Carissan devient professeur de mathématiques en 1896 et Eugène Carissan sort de Saint-Cyr. Pierre collabore à la revue de mathématiques amusantes *Le Sphinx-Œdipe* et s'intéresse à la construction d'une machine à congruences réalisée par son frère Eugène ; la machine étant peu performante, les deux frères imaginent des améliorations. Le travail s'interrompt pendant la Première Guerre Mondiale. Eugène reprend la fabrication après la guerre et la machine est finalement construite en 1919. Un article est publié dans le *Bulletin de la Société d'Encouragement à l'Industrie Nationale* en 1920 pour expliquer le principe et le fonctionnement de la machine.

Le problème des frères Carissan est la résolution d'équations en nombres entiers. L'idée est d'éliminer des valeurs impossibles de par leur résidu modulo m pour certaines valeurs du module m. Il s'agit bien d'une généralisation de la remarque de Fermat sur les « finales » car cela revenait à éliminer certaines valeurs à cause de leur résidu modulo 100. La machine des frères Carissan est donc utile pour résoudre un grand nombre d'équations diophantiennes[4] et en particulier, elle peut nous aider à trouver x et y tels que $N = x^2 - y^2$. Travaillons par exemple[5] modulo 7 et cherchons les résidus quadratiques modulo 7, c'est-à-dire les carrés modulo 7 :

x	0	1	2	3	4	5	6
x^2	0	1	4	2	2	4	1

Les résidus quadratiques modulo 7 sont 0, 1, 2, 4 et les non-résidus sont 3, 5, 6. Ceci signifie que, si un nombre est congru à 3, 5 ou 6 modulo 7, **il ne peut pas être un carré**. S'il est congru à 0, 1, 2 ou 4, tout est possible : il peut être un carré ou ne pas en être un. Reprenons notre problème de factorisation et cherchons à factoriser 250 507. Il s'agit donc de trouver x tel que $x^2 - 250\,507$ est un carré. On a : $N \equiv 5 \pmod 7$ donc $x^2 - 5$ doit être

[4] C'est-à-dire d'équations dont les inconnues sont des nombres entiers.

[5] Rappelons que deux entiers a et b sont congrus modulo 7 (noté $a \equiv b \pmod 7$) si et seulement si 7 divise $a - b$; tout entier est congru à son reste dans la division par 7 et on peut donc travailler avec les restes possibles, c'est-à-dire 0, 1, 2, 3, 4, 5 et 6. Enfin, les opérations « passent » aux congruences et si $x \equiv y \pmod 7$ alors $x^2 \equiv y^2 \pmod 7$.

un carré modulo 7 donc $x^2 - 5$ doit être congru à 0 ou 1 ou 2 ou 4 modulo 7. Donc x^2 doit être congru à 5 ou 6 ou 0 ou 2 modulo 7 ; comme x^2 est un carré, les seules valeurs possibles pour x^2 sont 0 ou 2 donc x doit être congru à 0 ou 3 ou 4 modulo 7. Les valeurs 0, 3, 4 sont appelées *valeurs possibles* modulo 7.

L'idée de la machine de Carissan est d'éliminer un grand nombre de valeurs de x en travaillant sur 14 modules simultanément. Examinons le principe de la machine de Carissan avec un modèle fonctionnant avec trois modules : 7, 9 et 15. Faisons avec 9 et 15 un travail semblable à celui effectué avec le module 7.

Carrés modulo 9 :

x	0	1	2	3	4	5	6	7	8
x^2	0	1	4	0	7	7	0	4	1

Carrés modulo 15 :

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
x^2	0	1	4	9	1	10	6	4	4	6	10	1	9	4	1

On a : $N \equiv 1 \pmod 9$ donc $x^2 - 1$ doit être un carré modulo 9 donc $x^2 - 1$ est congru à 0 ou 1 ou 4 ou 7 modulo 9 donc x^2 est congru à 1 ou 2 ou 5 ou 8 modulo 9 ce qui donne comme valeurs permises pour x modulo 9 : 1 ou 8.

Et enfin $N \equiv 7 \pmod{15}$ donc $x^2 - 7$ doit être congru à 0 ou 1 ou 4 ou 6 ou 9 ou 10. Donc x^2 est congru à 7 ou 8 ou 11 ou 13 ou 1 ou 2 donc les valeurs permises pour x modulo 15 sont : 1 ou 4 ou 11 ou 14.

Vous trouverez dans l'annexe 2 quatre pages, qui, photocopiées sur transparent, vous permettront de réaliser une machine de Carissan rétroprojetable[6] formée de trois disques matérialisant les restes de x dans les divisions par 7, 9 et 15. Plaçons sur chaque disque des gommettes sur les valeurs possibles pour x ; puis nous mettons la machine en position initiale correspondant à x = 501 car $501 = E(\sqrt{N}) + 1$. Nous alignons donc les valeurs 4, 6, 6 sur la ligne marquée **position initiale**. Tournons chaque disque d'un cran : les valeurs alignées sur la **position initiale** sont maintenant les valeurs de 502 modulo 7, 9 et 15. On continue à tourner et, lorsqu'on obtient trois gommettes alignées sur la **position initiale**, le nombre correspondant pour x a de bonnes chances de convenir car il est une valeur possible pour les modules 7, 9 et 15. Mais attention ! Ce n'est pas sûr et il faut vérifier à la main que cela marche bien.

Voici les valeurs successives obtenues :

mod7	4	5	6	0	1	2	3	4	5	6	0	1	2	**3**
mod9	6	7	8	0	1	2	3	4	5	6	7	8	0	**1**
mod15	6	7	8	9	10	11	12	13	14	0	1	2	3	**4**

Nous stoppons la machine après 14 essais (le premier compris) car nous obtenons trois valeurs permises. Essayons alors :

$$x = 501 + 13 = 514.$$

$$x^2 - N = 514^2 - 250\,057 = 13\,689 = 117^2.$$

$$\text{Donc } 250\,507 = (514 + 117)(514 - 117) = 631 \times 397.$$

La machine de Carissan permet de travailler sur 14 modules : 19, 21, 23, 26, 29, 31, 34, 37, 41, 43, 47, 53, 55 et 59. Elle comporte 14 couronnes comportant le nombre de plots correspondant à chacun de ces 14 modules. Pour résoudre notre problème de factorisation, il faut donc chercher les valeurs possibles de x dans chacun de ces modules. Ensuite, on place un capuchon sur les plots des valeurs possibles et on met la machine en position initiale pour le premier essai (501 dans notre exemple). Une manivelle permet de faire tourner les couronnes et lorsqu'on obtient 14 capuchons alignés, on tient une solution possible (mais pas sûre) : il faut alors faire un calcul « à la main » pour vérifier qu'on a bien une solution.

---

[6] Pour réaliser la machine rétroprojetable, attacher les trois disques grâce à une attache parisienne fixée en leur centre, puis fixer cette attache sur la ligne « position initiale » du quatrième transparent.

Avec sa machine, Carissan a montré que $2^{21}-1$ est premier et a factorisé 3 570 537 526 921 en 841 249 x 4 244 329 ; il n'a pas utilisé la méthode de Fermat mais des résultats sur la représentation de nombres entiers avec des formes quadratiques et en particulier la représentation des nombres sous forme de somme de deux carrés. Nous ne développerons pas ici ces théories, qui feront peut-être l'objet d'un autre conte du lundi.

La méthode du crible quadratique

Dans l'article de *Pour la Science* cité en bibliographie, Johannes Buchmann explique une méthode moderne de factorisation utilisant les mêmes idées. Si on cherche à factoriser un nombre N, on cherche deux nombres x et y tels que $x^2-y^2\equiv 0$ (modN) avec $x\neq \pm y(\mathrm{mod}\,N)$. (Remarquons que cela n'est possible que si N n'est pas premier car, si N est premier, « N divise x^2-y^2 » entraîne « N divise x –y ou N divise x + y »). Si N divise x^2-y^2 sans diviser x – y ni x + y alors un diviseur propre p de N divise x – y et un autre diviseur propre q de N divise x + y . Donc P.G.C.D.(x – y, N) ≠ 1 et il suffit de calculer P.G.C.D.(x – y, N) par l'algorithme d'Euclide pour trouver un diviseur de N différent de 1 et de N. Le problème est donc de trouver x et y convenables.

La méthode du crible quadratique consiste à choisir une base de nombres premiers $\{p_1,p_2,p_3,...,p_n\}$ avec laquelle on va travailler. Dans une première étape, on cherche des nombres a tels que a^2 est « proche » de N (dans un sens qu'on précisera plus tard) tels que a^2-N admette uniquement les nombres de la base choisie comme facteurs premiers. Nous allons appliquer la méthode à N = 125 249. La base choisie est $\{2,3,5,7,11,13\}$. E(√N) = 353 donc on prendra a « proche » de 353. Le tableau suivant montre le « crible » appliqué : pour chaque valeur de a, on a mis dans la ligne de chaque facteur premier choisi la puissance à laquelle il intervient dans la décomposition de a^2-N ; la case reste vide s'il n'intervient pas ; enfin, dans la dernière ligne, figure le facteur restant quand on a divisé a^2-N par tous les nombres premiers de la base ; si ce nombre est 1, alors a nous convient car a^2-N admet comme seuls diviseurs premiers ceux de la base choisie, sinon la valeur est à rejeter.

a	347	348	349	350	351	352	353	354	355	356	357
a^2-N	-4840	-4145	-3448	-2749	-2048	-1345	-640	67	776	1487	2200
-1	-1	-1	-1	-1	-1	-1	-1				
2	2^3		2^3		2^{11}		2^7		2^3		2^3
3											
5	5	5					5				5^2
7											
11	11^2										11
13											
	1	829	431	2749	**1**	269	**1**	354	97	1487	**1**

Il y a donc dans ce cas 4 valeurs convenables. On écrit alors les décompositions obtenues :

$$L_1 : 347^2 - N = (-1)\times 2^3\times 5\times 11^2$$
$$L_2 : 351^2 - N = (-1)\times 2^{11}$$
$$L_3 : 353^2 - N = (-1)\times 2^7\times 5$$
$$L_4 : 357^2 - N = 2^3\times 5^2\times 11$$

Il faut ensuite choisir certaines lignes qu'on va multiplier entre elles ; le but est d'obtenir dans le membre de droite uniquement des exposants pairs. Pour cela on résout un système d'équations linéaires dans **Z/2Z** : on affecte en effet à chaque ligne un coefficient λ_i égal à 1 si on prend la ligne et à 0 si on ne la prend pas ; l'exposant de 2 obtenu dans le membre de droite par la multiplication des lignes est alors $3\lambda_1+11\lambda_2+7\lambda_3+3\lambda_4$; il faut donc trouver un quadruplet $\{\lambda_1,\lambda_2,\lambda_3,\lambda_4\}$ tel que les exposants obtenus pour –1 et pour 2, 5, 11(seuls nombres premiers intervenant ici) soient tous pairs, c'est-à-dire nuls dans **Z/2Z** . De plus, $3\lambda_1+11\lambda_2+7\lambda_3+3\lambda_4$ est pair si et seulement si $3\lambda_1+11\lambda_2+7\lambda_3+3\lambda_4\equiv 0(\mathrm{mod}\,2)$ c'est-à-dire si $\lambda_1+\lambda_2+\lambda_3+\lambda_4=0$ dans **Z/2Z**. On obtient ainsi un système de 4 équations à 4 inconnues dans **Z/2Z**.

$$\begin{cases} \lambda_1 + \lambda_2 + \lambda_3 = 0 \\ \lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 = 0 \\ \lambda_1 + \lambda_3 = 0 \\ \lambda_4 = 0 \end{cases}$$

On a réduit tous les coefficients modulo 2. La résolution du système donne : $\begin{cases} \lambda_2 = 0 \\ \lambda_4 = 0 \\ \lambda_1 + \lambda_3 = 0 \end{cases}$ et on choisit comme solution $\begin{cases} \lambda_1 = \lambda_3 = 1 \\ \lambda_2 = \lambda_4 = 0 \end{cases}$. La multiplication des lignes L_1 et L_3 donne alors :

$(347^2 - N)x(353^2 - N) = (-1)^2 x\ 2^{10} x\ 5^2 x\ 11^2$

Donc : $347^2 \times 353^2 \equiv (2^5 \times 5 \times 11)^2$ (modN)

Or $347 \times 353 \equiv 122491 \equiv -2758$ (modN) et $2^5 \times 5 \times 11 = 1760$. On obtient alors : $2758^2 \equiv 1760^2$ (modN) . Donc N divise $2758^2 - 1760^2 = (2758 + 1760)x(2758 - 1760)$ sans diviser l'un des facteurs. Un diviseur propre de N divise alors $2758 - 1760 = 998$. On applique l'algorithme d'Euclide pour trouver P.G.C.D.(N,998).

$$125\,249 = 125 \times 998 + 499$$

$$998 = 2 \times 499$$

On a : P.G.C.D.(N,998) = 499. On tient un diviseur de N.

$$125\,249 = 499 \times 251.$$

Pour factoriser un nombre de 50 chiffres, il faut une base de facteurs premiers comportant 3000 nombres premiers ; il en faut 51 000 pour un nombre de 100 chiffres.

Le problème de la factorisation des grands nombres et du temps de calcul pour y parvenir est revenu sur le devant de la scène avec la cryptographie moderne : la sécurité du système R.S.A. repose sur la difficulté (présumée) de factoriser rapidement de très grands nombres[7].

[7] voir conte du lundi p 31 dans ce numéro.

Annexe 1 : somme des diviseurs d'un nombre

On note : $\sigma(N) = \sum_{d/N} d$ la somme des diviseurs d'un nombre entier N (y compris N).

Si le nombre p est premier, on a $\sigma(p) = 1 + p$ et $\sigma\left(p^{\alpha}\right) = 1 + p + p^2 + ...p^{\alpha}$.

Si p et q sont deux nombres premiers distincts, on a alors :

$$\begin{aligned}\sigma\left(p^{\alpha}\right) \times \sigma\left(q^{\beta}\right) &= (1 + p + ... + p^{\alpha}) \times (1 + q + ... + q^{\beta}) \\ &= 1 + p + ... + p^{\alpha} + q + pq + ...p^{\alpha}q + ...q^{\beta} + q^{\beta}p + ...q^{\beta}p^{\alpha} \\ &= \sum_{\substack{0 \le i \le \alpha \\ 0 \le j \le \beta}} p^i q^j = \sigma\left(p^{\alpha} q^{\beta}\right)\end{aligned}$$

On obtient ainsi, lorsque

$N = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_n^{\alpha_n}$ où les p_i sont premiers avec $p_i \neq p_j$, $\sigma(N) = \sigma\left(p_1^{\alpha_1}\right) \times \sigma\left(p_2^{\alpha_2}\right) \times ... \times \sigma\left(p_n^{\alpha_n}\right)$

Et de même, si m et n sont premiers entre eux : σ(m.n) = σ(m)σ(n).

On peut alors s'attaquer au problème posé par Mersenne à Fermat et à la réponse[8] de celui-ci dans sa lettre du 7 avril 1643. On cherche la somme des diviseurs de

N = 241 748 364 800 000 x 11 x 19 x 43 x 61 x 83 x 169 x 223 x 331 x 379 x 601 x 757 x 1201 x 7019 x 823 543 x 616 318 177 x 6561 x 100 895 598 169

241 748 364 800 000 = 2^{36} x 5^5 et il n'y a pas d'autre facteur 2 ou 5 dans N. En fait, les facteurs de N donnés par Mersenne sont premiers deux à deux donc on cherche la somme des diviseurs de chacun d'eux pour obtenir la somme des diviseurs de N.

$\sigma\left(2^{36}\right) = 1 + 2 + ...2^{36} = 2^{37} - 1 = 137438953471 = 223 \times 616318177$ Or 616 318 177 est un facteur premier qu'on retrouve dans N, ce qui va faciliter le calcul de $\frac{\sigma(N)}{N}$.

σ(11) = 12 =2^2x3

σ(19) = 20 = 2^2x 5

σ(43) = 2^2 x 11

σ(61) = 62 = 2 x 31

σ(83) = 84 = 2^2 x 3 x 7

σ(169) = σ(13^2) = 1 + 13+ 13^2 = 3 x 61

σ(223) = 224 = 2^5 x 7

σ(331) = 332 = 2^2 x 83

σ(379) = 380 = 2^2 x 5 x 19

σ(601) = 602 = 2 x 7 x 43

σ(757) = 758 = 2 x 379

σ(961) = σ(31^2) = 1 + 31 + 31^2 = 993 = 3 x 331

σ(1201) = 1202 = 2 x 601

σ(7019) = 7020 = 2^2 x 3^3 x 5 x 13

σ(6561) = σ(3^8) = (3^9 – 1)/2 = 13 x 757

σ(823 543) = σ(7^7) = (7^8 – 1)/6 = 2^5 x 5^2 x 1201

σ(616 318 177) = 616 318 178 = 2 x 7^3 x 898 423

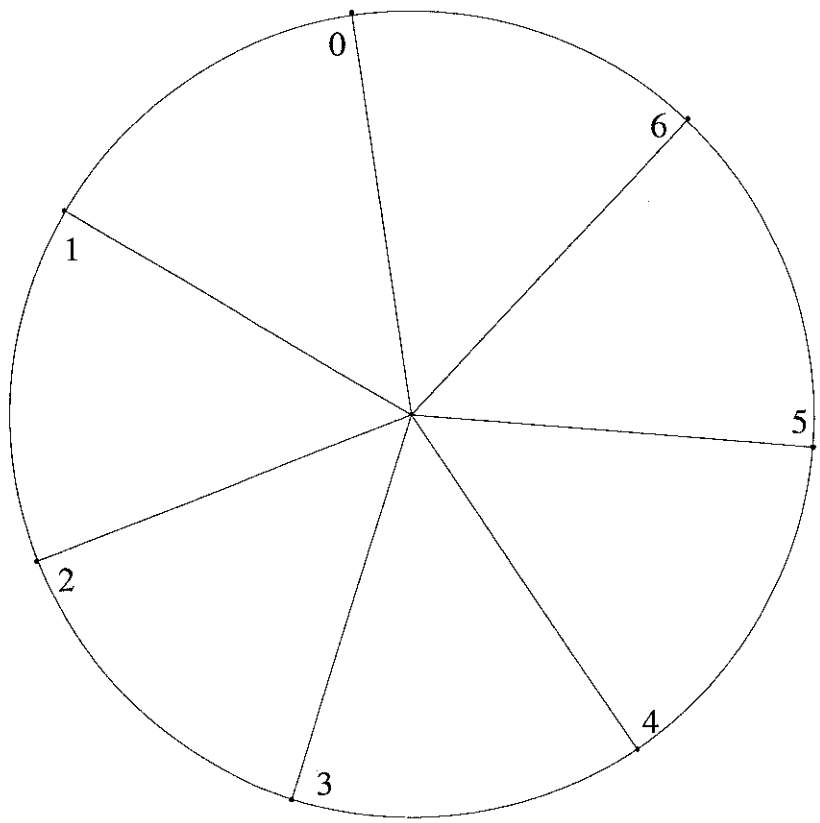
[8] La méthode suivie est celle suggérée par Tannery dans l'édition des œuvres de Fermat citée en bibliographie.

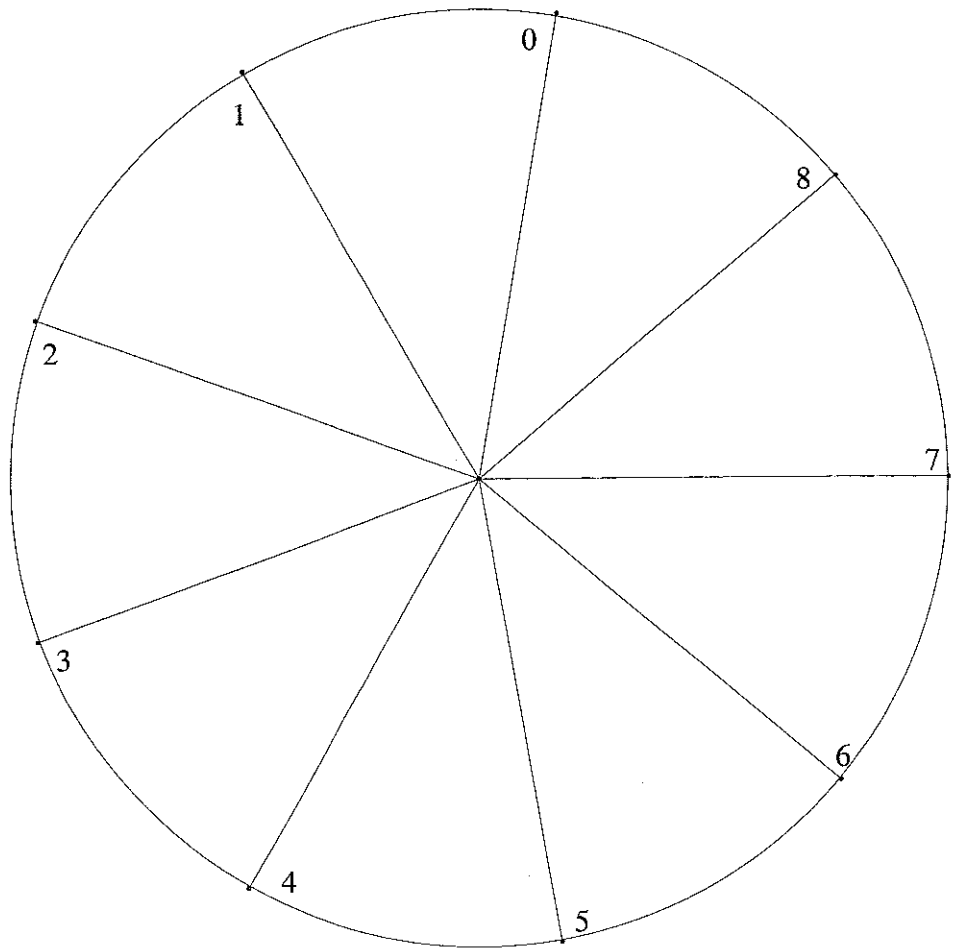
Reste à trouver σ(100 895 598 169)et donc la décomposition de 100 895 598 169. Or tous les facteurs trouvés dans les sommes de diviseurs déjà calculés sont des facteurs de N sauf 898 423. Fermat a dû raisonner comme un bon élève qui, devant un problème qu'on lui demande de résoudre, pense qu'il doit être résoluble ! Or, ici, si on veut pouvoir calculer σ(N)/N, il serait bien pratique que 898 423 divise N. Essayons donc de voir s'il divise le dernier facteur de N. Or, justement, en essayant, on trouve la décomposition de ce fameux 100 895 598 169 , c'est-à-dire : 898 423 x 112 303. Par la même occasion, terminons le calcul de la somme des diviseurs :
σ(898 423) = 898 424 = 2^4 x 112 303 et σ(112 303) = 112 304 = 2^4 x 7019
On peut dire que cela tombe merveilleusement bien puisqu'on retrouve des facteurs de N. On peut maintenant trouver σ(N)/N = 2 x 3 = 6.

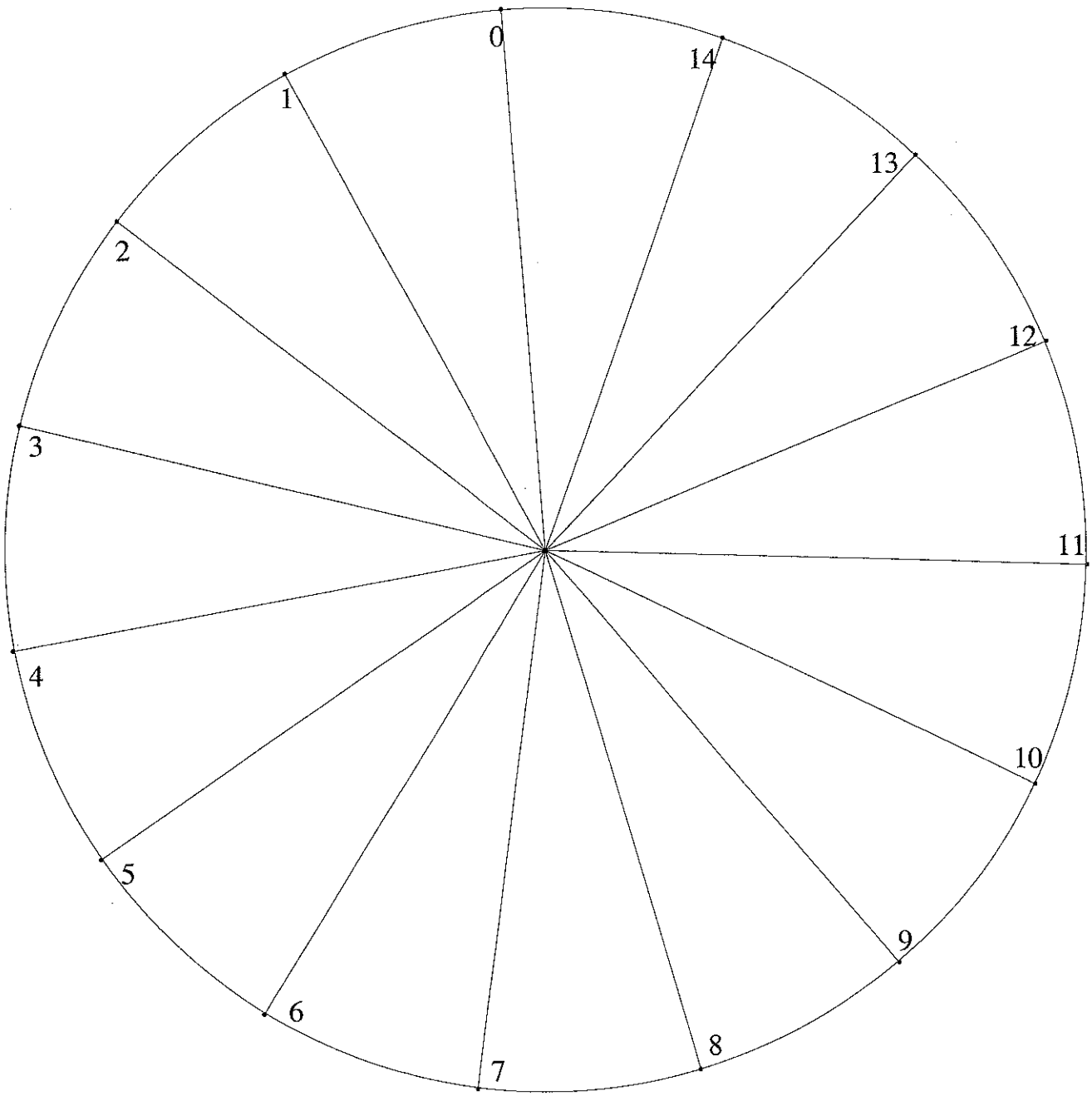
Fermat, lui, s'occupe de la somme des parties aliquotes, c'est-à-dire de $s(N) = \sum_{\substack{d/N \\ d \neq N}} d = \sigma(N) - N$. Donc s(N) = 5N ; N est sous-quintuple de ses parties aliquotes et, en cours de calcul, on a trouvé la factorisation de 100 895 598 169.

Annexe 2 : machine de Carissan rétroprojetable à trois disques

Position initiale


0
6
1
5
2
4
3


0
1
8
2
7
3
6
4
5


0
14
13
12
11
10
9
8
7
6
5
4
3
2
1

Bibliographie

P. FERMAT *Œuvres*, éd. Tannery et Henry, 1894, pp. 257-258

E. CARISSAN *Machine à résoudre les congruences*, Bulletin de la Société d'Encouragement à l'Industrie Nationale, n°132, 1920.

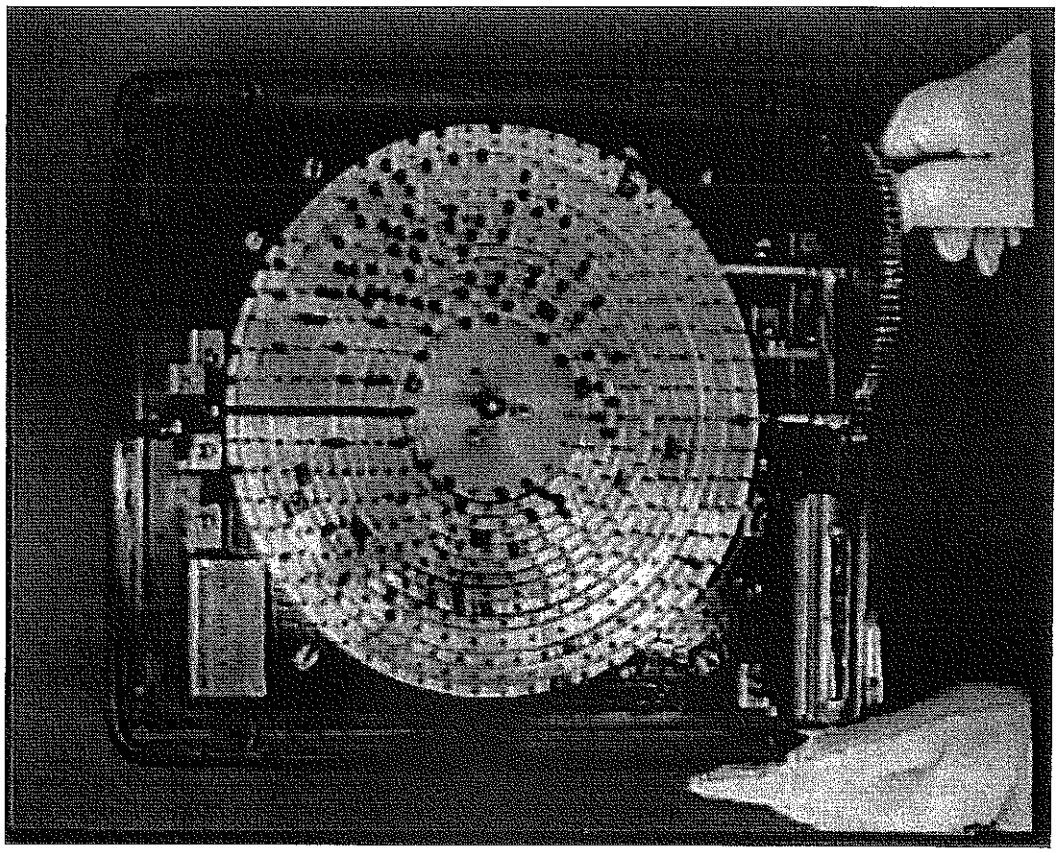
F. MORAIN *La machine de Carissan*, Pour la Science, janvier 1998.

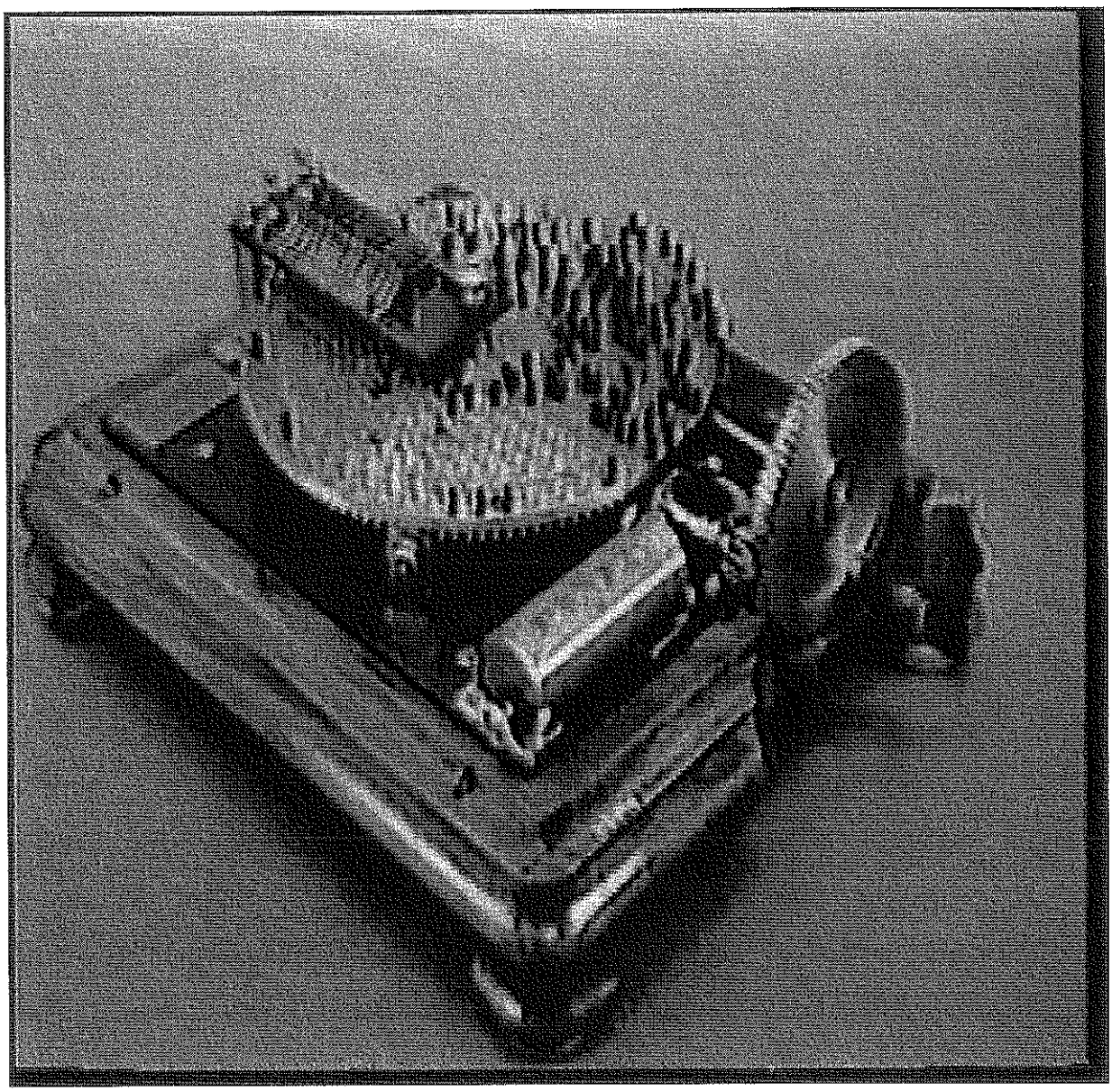
F. MORAIN, J.O. SHALLIT, H.C. WILLIAMS *La machine à congruences*, La Revue n°14, Musée des Arts et Métiers Editions, mars 1996.

J. BUCHMANN *La factorisation des grands nombres*, Pour la Science, n°251, septembre 1998.

J.P. DELAHAYE *La cryptographie R.S.A. vingt ans après*, Pour la Science, n°267, janvier 2000.

Un film d'une quinzaine de minutes a été réalisé sur la machine de Carissan avec le Musée des Arts et Métiers ; ce film peut être emprunté à la bibliothèque de l'I.R.E.M. Paris VII.





CONTE DU LUNDI I

ARITHMETIQUE ET CODES SECRETS
Un coup d'œil historique

Martine Bühler

Ce conte du lundi doit beaucoup à mes lectures, diverses mais toujours passionnées, sur l'histoire de la cryptographie. Vous trouverez bien sûr à la fin de l'article une bibliographie, mais je tiens à signaler ma dette envers deux ouvrages et un article : les livres de S. Singh et J. Stern et l'article de R. Noirfalise dans *Repères*.

Les premiers systèmes de codes

Jules César a utilisé divers types de codes secrets. Dans *La Guerre des Gaules*[1], il raconte qu'il envoya un message à Cicéron dans lequel les lettres latines étaient remplacées par les lettres grecques correspondantes ; cela suffisait à rendre illisible le message par l'ennemi (pas assez cultivé pour connaître le grec !) mais limpide pour Cicéron. Jules César, conquérant fameux, eut recours à plusieurs codages ; dans *La Vie des douze Césars*[2], Suétone en décrit un autre : on remplace chaque lettre du message par la lettre placée trois rangs après elle dans l'alphabet.

Dans les deux cas, il s'agit d'un codage « monoalphabétique » ou « monograhique ». Chaque lettre est remplacée par un symbole ; dans les deux exemples donnés il s'agissait d'une autre lettre de l'alphabet ou d'une lettre grecque, mais ce pourrait aussi être un symbole n'ayant aucune autre signification ou un dessin.

Mettons-y tout de suite de l'arithmétique, bien que cela soit inutile à ce stade, car, tout ou tard, il faudra bien en venir là !

Chaque lettre de l'alphabet est associé à un nombre comme dans le tableau ci-dessous :

Lettre	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
Nombre associé	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Définir un codage monoalphabétique revient à définir une fonction arithmétique de $\{0,1,2,...,23,24,25\}$ dans lui-même ou, pour parler un langage plus moderne de $\mathbb{Z}/26\mathbb{Z}$ dans lui-même. Par exemple, le deuxième procédé de Jules César correspond à l'opération suivante : si x est le nombre associé à une des lettres du message, on définit $f(x) \equiv x+3 (\mathrm{mod}\, 26)$ avec $0 \leq f(x) \leq 25$. La lettre cryptée est la lettre associée à f(x) dans le tableau ci-dessus. Les exercices 1 et 2 de l'annexe 1 proposent des codages définis par des fonctions arithmétiques simples.

En fait, on peut définir une permutation des lettres sans congruences, en donnant par exemple un tableau de correspondance entre lettres « en clair » et lettres « cryptées » ; mais encore faut-il être sûr que ce tableau ne tombera pas entre les mains de l'ennemi. Aussi a-t-on souvent utilisé des mots-clefs ou des phrases-clefs. Par exemple, décidons de prendre comme mot-clef MATHEMATIQUES ; ré-écrivons-le sans répétition MATHEIQUS ; nous obtiendrons le tableau de correspondance entre lettres en clair et lettres cryptées de la manière suivante :

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

On a commencé par écrire le mot-clef sans répétition dans le tableau et on a continué à partir de la dernière lettre en suivant l'ordre alphabétique sans répétition. Il suffit donc d'apprendre le mot-clef par cœur et on peut communiquer en sécurité ; on peut même choisir une phrase-clef assez longue. Comme il y a 26 ! permutations

[1] Cesar *De bello Gallico (La Guerre des Gaules)* Traduction L.A. Constans Les Belles Lettres 1937.

[2] Suetone *De Vita Caesarum (Laa Vie des Douze Cesars)* Traduction Henri Ailloud Les Belles Lettres 1961.

possibles des lettres de l'alphabet, ce type de codages paraît difficile à déchiffrer sans le mot-clef ou la fonction arithmétique de codage. Ce mode de communication codée fut donc employé et considéré comme sûr pendant fort longtemps.

Un progrès décisif dans le déchiffrement des messages cryptés fut accompli dans la civilisation arabo-islamique ; les savants arabes se sont intéressés à la linguistique et découvrirent que certaines lettres sont plus utilisées que d'autres. Al Kindi rédigea au IX^{ème} siècle un *Manuscrit sur le déchiffrement des messages cryptographiques* où il utilise cette particularité. Cette méthode porte le nom d'analyse des fréquences. Transposons-la au français : les trois lettres les plus employées en français sont les lettres E, A et I[3] ; en présence d'un texte crypté (dont on a de bonnes raisons de penser qu'il est écrit en français), on compte la fréquence d'apparition de chaque lettre dans le texte crypté. Les trois lettres les plus répandues sont probablement mises pour E, A et I (mais éventuellement dans un ordre différent). On repère également les couples fréquents avec ces trois lettres cryptées : par exemple, si on pense que la lettre H code la lettre E, on repérera dans le texte crypté les lettres qui suivent le plus fréquemment le H et on fera l'hypothèse qu'elles sont mises pour T ou N. Ensuite, on emploie une technique bien connue des amateurs de mots croisés consistant à deviner des mots dont on connaît seulement certaines lettres.

Cette technique permet de venir à bout de tout message crypté grâce à un système monoalphabétique, à condition qu'il soit suffisamment long –une quarantaine de lettres- et composé de mots « normaux ». La méthode fonctionne également si on choisit de remplacer chaque lettre, non pas par une autre lettre, mais par un symbole sans signification particulière (par exemple un rond pour A, un carré pour B, etc.) ; il suffit d'appliquer la méthode des fréquences à ces symboles. Un exemple de ce type de déchiffrement est donné dans *Les hommes dansants*, une nouvelle d'Arthur Conan Doyle où l'on voit Sherlock Holmes déchiffrer des messages où chaque lettre est codée par un « bonhomme » dans une position différente (mais l'analyse est faite en tenant compte de la fréquence des lettres en anglais)[4].

L'Europe à la même époque accuse un retard certain en cryptographie. Le premier livre traitant du sujet est un livre de Bacon au XIII^{ème} siècle . La cryptographie se répand au XIV^{ème} siècle et la cryptanalyse suit au XV^{ème} siècle. On essaie des systèmes dérivés du codage monoalphabétique en le compliquant, mais ces systèmes ne résistent pas à une amélioration de l'analyse des fréquences.

Le système de Vigenère

Afin d'éviter le déchiffrement par analyse statistique, Alberti propose en 1460 d'alterner deux alphabets cryptés par décalage de lettres : par exemple, les lettres ayant un rang pair dans le message en clair seront décalées de 7 et celles de rang impair seront décalées de 11 ; le mot MESSAGE devient donc TPZDHRL. Ainsi la même lettre S est codée différemment. C'est un début de réponse des cryptographes (ceux qui cherchent à rendre les communications illisibles par un supposé espion) aux cryptanalystes (ceux qui cherchent à déchiffrer des messages secrets qui ne leur sont pas *a priori* destinés). Le même type de démarche va mener Vigenère(1523-1596) au système qui porte son nom, qu'il décrit dans son *Traité des chiffres*(1586). Les correspondants choisissent un mot-clef qu'ils gardent secret, par exemple le mot ROSE. Le code consiste à utiliser 4 (nombre de lettres du mot-clef) alphabets translatés : la première lettre du message est translaté de 17 (rang de la lettre R – première lettre du mot-clef – dans l'alphabet « normal »), la deuxième lettre du message est translaté de 14 (rang de O), la troisième de 18 et la quatrième de 4 ; ensuite on recommence le cycle. Par exemple, cryptons les mots CODE SECRET avec le mot-clef ROSE.

Le tableau suivant nous aidera :

---

[3] En fait, si on consulte des tables de fréquences des lettres en français dans différents ouvrages, on s'aperçoit qu'elles ne concordent pas entièrement ; par exemple, les lettres les plus fréquentes peuvent être E et S au lieu de E et A. Le mieux est d'établir sa propre table à partir de textes du même type que ceux qu'on veut déchiffrer ; en effet, un texte « militaire » ne présentera pas les mêmes fréquences qu'un roman ou un texte scientifique, car il n'emploie ni le même style, ni les mêmes mots les plus fréquents.

[4] Voir aussi *Le scarabée d'or* d'Edgar Allan Poe.

Mot-clef	R 17	O 14	S 18	E 4	R 17	O 14	S 18	E 4	R 17	O 14
Lettre en « clair »	C	O	D	E	S	E	C	R	E	T
Nombre associé	2	14	3	4	18	4	2	17	4	19
Nombre « translaté »	19	2	21	8	9	18	20	21	21	7
Lettre « cryptée »	T	C	V	I	J	S	U	V	V	H

Ce système permet d'éviter l'analyse de fréquences : la lettre E par exemple est cryptée de trois manières différentes : I, puis S et enfin V. De plus, une même lettre cryptée peut représenter des lettres différentes : V représente D, puis R, puis E. Le système n'est cependant pas utilisé immédiatement car il est jugé trop compliqué à mettre en œuvre ; on lui préfère des codes monoalphabétiques ou dérivés plus simples. Mais au XVIII^{ème} siècle, la cryptanalyse se développe et devient un métier ; les codes monoalphabétiques ne résistent plus au déchiffrement ; les cryptographes se résignent à utiliser le système de Vigenère malgré sa complexité. L'usage des télégraphes au XIX^{ème} siècle accélère la course aux codes « sûrs ». Ce type de codage sera cependant brisé par l'Anglais Babbage au XIX^{ème} siècle. Reprenons l'exemple ci-dessus, avec le mot-clef ROSE : un mot de 3 lettres peut être crypté de 4 manières différentes : par décalages successifs de 17, 14, 18 (correspondant aux rangs des lettres R, O, S dans l'alphabet) si le rang de la première lettre de ce mot dans le message en clair est congru à 1 modulo 4, ou bien par décalages successifs de 14, 18, 4 (correspondant aux rangs des lettres O, S, E) si le rang de la première lettre est congru à 2 modulo 4, ou bien par décalages successifs de 18, 4, 17 (rangs de S, E, R), ou bien par décalages successifs de 4, 17, 14 (rangs de E, R, O). Si ce mot intervient 5 fois dans le message, alors il sera codé 2 fois de la même façon (hé oui ! le fameux principe des tiroirs intervient aussi dans les codes secrets !). Ce qui précède est bien sûr valable pour toute suite de lettres intervenant au moins 5 fois dans le message (5, c'est-à-dire une fois de plus que le nombre de lettres du mot-clef). Venons-en à la méthode de cryptanalyse de Babbage : lorsque le message est suffisamment long, on recherche des séquences de lettres se reproduisant plusieurs fois dans le message crypté. Soit c'est une coïncidence (ce qui est peu probable si on choisit des séquences de 4 lettres ou plus), soit il s'agit d'une même suite de lettres cryptée plusieurs fois de la même façon ; le nombre de lettres séparant deux séquences identiques est alors un multiple du nombre de lettres du mot-clef. Si plusieurs séquences se répètent après des intervalles de n_1, n_2, n_3..., alors P.G.C.D.(n_1,n_2,n_3,...) ou un de ses diviseurs est sans doute le nombre de lettres du mot-clef. Si on a trouvé que ce nombre est d par exemple, on regarde uniquement les lettres du message crypté dont le rang est congru à 1 modulo d et on leur applique la méthode d'analyse des fréquences (qui marche d'autant mieux qu'on connaît la nature de la permutation appliquée aux lettres de l'alphabet : une simple translation), on recommence avec les lettres de rang congru à 2 modulo d, etc. Un exemple de cryptanalyse par cette méthode est proposé dans l'annexe 2.

Babbage n'a pas publié son travail, qui n'est connu que par des papiers non publiés retrouvés au XX^{ème} siècle. Un autre cryptanalyste, Kasiski, est arrivé ultérieurement au même résultat et a publié ses travaux en 1863.

Le cryptage mécanisé

Il faut donc, pour rendre le message indéchiffrable, éviter ces répétitions de séquences de lettres ; les cryptographes trouvent la parade : la clef doit être aussi longue que le message. On peut par exemple choisir les paroles d'une chanson, commode à mémoriser. Mais les cryptanalystes sont gens tenaces et inventifs : ils imaginent la méthode des « mots probables », qu'on retrouvera utilisée de main de maître par les services secrets anglais pendant la deuxième guerre mondiale. L'idée est la suivante : le message contient sûrement des mots courants, par exemple « les », « une », etc. On place ces mots au hasard dans le message crypté et on regarde ce que cela donne pour les lettres de la clef. Si les mots courants sont mal placés, il y a de fortes chances que la suite de lettres obtenue pour la clef soit improbable (par exemple ZGT), alors que, si le mot courant a été bien placé, les lettres du mot-clef semblent cohérentes (par exemple MAT) ; la suite ressemble aux techniques

empiriques des cruciverbistes : on essaie de compléter les lettres obtenues pour obtenir des mots qui ont un sens (par exemple, MAT pourraient être le début de MATHEMATIQUES) et on retourne au message codé pour voir ce que cela donne ; si le décodage avec le mot-clef supposé a un sens, on ne s'est probablement pas trompé ; sinon faisons d'autres essais. Le va-et-vient entre la clef et le message codé allié à la technique « cruciverbiste » permet le déchiffrement.

La seule solution pour rendre le message indéchiffrable est de prendre comme clef une suite de lettres choisies au hasard aussi longue que le message (et n'ayant donc aucun sens). Cette fois, la cryptanalyse est impossible : en effet, supposons qu'on dispose d'un message codé de cette manière (mais sans la clef évidemment). Pour tout message en clair ayant le même nombre de lettres, on peut trouver une clef telle que le cryptage avec cette clef donne le message crypté de départ ; parmi tous ces messages possibles, on ne peut pas savoir lequel est le bon car, la clef ayant été choisie au hasard et n'ayant aucun sens, on ne peut pas s'appuyer sur elle comme précédemment pour vérifier nos hypothèses de déchiffrement. Ce système est donc imparable ! Est-ce à dire qu'il est parfait ?

En fait, ses défauts proviennent de la complexité de sa mise en œuvre. Tout d'abord, il faut une clef différente pour chaque message. Si le cryptanalyste dispose de deux messages différents codés avec la même clef, il peut utiliser sa méthode des « mots probables » : il place au hasard des mots courants dans le premier message, en déduit un morceau de clef possible, puis décrypte une partie du deuxième message avec ce morceau de clef. Si celui-ci a un sens, il essaie de compléter les mots par la technique « cruciverbiste », puis revient au premier message avec une clef complétée et ainsi de suite : le va-et-vient entre les deux messages permet le déchiffrement. Il faut donc établir un grand nombre de longues suites de lettres aléatoires à l'avance. L'expéditeur et le destinataire des messages dispose chacun de deux « carnets de code » identiques ayant des centaines de pages, chaque page comportant une suite aléatoire de centaines de lettres. Le premier message est codé avec la page numéro 1, le deuxième message avec la page numéro 2, etc. On imagine la lourdeur du procédé, le codage et le décodage n'étant par ailleurs pas spécialement rapides ! Et que dire du problème de la distribution des clefs ? Si l'ennemi s'empare d'un carnet de codes (imaginez une armée en campagne où chaque compagnie a son spécialiste chargé de décoder les messages de l'Etat-Major possédant donc le carnet commun), les messages codés seront aussi limpides pour lui que des messages en clair. Ce problème de distribution des clefs est récurrent en cryptographie et nous verrons qu'il ne sera réglé qu'avec le concept de clef publique et l'irruption de l'arithmétique sur le devant de la scène au vingtième siècle.

La complexité du codage est également un obstacle majeur pour des Etats ayant un nombre important de messages à transmettre chaque jour. Dans les années vingt, un inventeur allemand, Scherbius, invente une machine permettant le brouillage automatique des messages : la machine Enigma. Elle dispose d'un clavier ordinaire de machine à écrire sur lequel on tape le message en clair ; chaque lettre est automatiquement décalée pour donner le message crypté. Le décalage change à chaque lettre car la machine possède plusieurs « brouilleurs » électriques connectés les uns aux autres (voir illustration, p.54). Le récepteur et l'émetteur doivent disposer de deux machines identiques et la mettre sur la même position de départ pour communiquer en toute sécurité. Ainsi, les carnets de codes ne servent plus qu'à transmettre un message très court par jour : la position initiale de la machine Enigma. A partir de là, codages et décodages se font automatiquement ; même si l'ennemi s'empare d'une machine, il ne pourra pas décoder les messages, car il ne connaît pas la position initiale (et il y en a de plus en plus : 10^{16} au départ et cela augmente dans des proportions astronomiques avec le perfectionnement d'Enigma).

Dans les années trente, l'armée allemande se dote de 30 000 machines Enigma.

Dès 1931, la France se procure les plans de la machine Enigma, mais les services secrets français n'en font aucun usage ; ils les font cependant parvenir aux services de renseignements polonais, qui, se sentant sans doute plus directement menacés par les visées allemandes, vont faire de réels efforts pour déchiffrer Enigma. La mécanisation du système de chiffrement les incite à recruter des scientifiques pour ce travail. Rejewski, mathématicien polonais, analyse les différents aspects du fonctionnement d'Enigma et attaque le système à partir de la répétition du message-clef : le carnet de codes ne contient que la position initiale du jour, servant à réceptionner le message codé ; mais celui-ci n'est pas codé avec la position initiale du carnet de codes, car la multiplication des messages codés de la même façon dans la journée faciliterait la cryptanalyse. Simplement, le message commence par un « message-clef » donnant la position initiale des trois rotors : la suite du message est codé avec cette position initiale, les autres réglages restant ceux du carnet de codes. La position des trois rotors

est donnée par une suite de trois lettres, par exemple PFK, et, pour éviter les erreurs à la réception, ce groupe de trois lettres est émis deux fois : le message-clef comporte donc six lettres PFKPFK, codées avec la position initiale donnée par le carnet de codes. Or, cette répétition apporte une faiblesse dans la sûreté du codage ; en effet, les deux groupes de trois lettres PFK sont codés de deux manières différentes car les rotors avancent d'un cran à chaque lettre codée. Ainsi PFKPFK est codée par exemple LTIHVC ; la lettre P est codée successivement par L et H ; les lettres L et H sont donc liées entre elle par le fait que, avec la position initiale choisie, elles codent toutes deux la même lettre , l'une au rang 1 du message et l'autre au rang 4. Si je ne connais pas la position initiale, je sais néanmoins que ces deux lettres sont liées par cette position initiale ; de même pour les lettres T et V, H et C. Rejewski a alors l'idée d'établir un « répertoire » des liaisons : une position initiale étant donnée, quelles sont les liaisons qu'elle induit sur les couples de lettres de l'alphabet ? Les Polonais construisent une version mécanisée de ce répertoire, permettant d'accélérer le décryptage, de la même façon que les machines Enigma permettent d'accélérer le cryptage. Cependant, en 1938, la machine passe à 5 rotors : on commence par choisir 3 rotors parmi les 5 possibles avant de les placer dans leur position initiale ; cela multiplie par 10 le nombre de possibilités et met à mal les méthodes polonaises. En 1939, la Pologne offre aux Alliés deux machines Enigma et les plans des machines à décrypter de Rejewski.

En Angleterre, les services de renseignements lance l'opération «Ultra», transportant à Bletchley Park (Buckinghamshire) le « Government Code and Cypher School », chargé d'intercepter et de décrypter les messages ennemis. On recrute intensément parmi les plus brillants spécialistes : mathématiciens, historiens, linguistes, spécialistes de japonais et d'allemand,...Alan Turing arrive à Bletchley en septembre 1939. Les Anglais travaillent à partir des méthodes élaborées par les Polonais. Mais en 1940, les Allemands suppriment la répétition du message-clef. Turing opte pour la méthode des « mots probables » ; il recherche des formules courantes (par exemple BULLETIN METEO) pour faire des hypothèses quant au déchiffrement, puis élimine des liaisons impossibles ; il traduit ses raisonnements en un système de relais électriques qui permet d'explorer rapidement les différentes hypothèses et de ne retenir que celles qui sont plausibles. Les Britanniques réussissent ainsi à déchiffrer les messages allemands.

Après la seconde guerre mondiale, le développement de l'informatique impulse de nouvelles recherches en cryptographie. Un message est transformé en une suite de 0 et de 1 et il s'agit de crypter cette suite . Les Etats-Unis adoptent le Data Encryption Standard (DES) à la fin des années soixante-dix. Le DES sépare le message en tranches de 64 bits sur lesquelles on opère des transformations définies par une clef de 64 bits (une suite de 64 termes formée de 0 et de 1 c'est-à-dire un grand nombre écrit en système binaire). Le DES est resté en service jusqu'à nos jours ; le *Monde* annonçait dernièrement qu'il allait être remplacé par un nouveau système inventé par des cryptographes belges (voir article du *Monde* dans l'annexe 5). Cependant, le DES n'échappe pas au problème signalé plus haut de la distribution des clefs.

L'arithmétique au secours de la cryptographie

Avant d'expliquer en quoi consiste le cryptage R.S.A. (acronyme de ses inventeurs Rivest, Shamir, Adleman), devenu célèbre au vingtième siècle, expliquons un système de codage par exponentiation, qui, à ma connaissance, n'a pas été utilisé, mais qui est une bonne introduction aux systèmes actuels. Ce système est très bien expliqué dans l'article de Robert Noirfalise cité en bibliographie.

On choisit un nombre premier p et un nombre entier e tel que e est premier avec p-1. Le couple (p,e) constituera notre clef de codage tenue secrète. Il est hors de question de coder lettre à lettre un message, car ce procédé ne résisterait pas à l'analyse des fréquences. On commence donc par grouper les lettres du message en blocs de m lettres. Un bloc correspond alors à un nombre de la manière suivante : nous avons vu qu'on peut associer à chaque lettre un nombre entre 0 et 25 (qu'on peut considérer comme un nombre à deux chiffres, quitte à rajouter un zéro pour les dizaines éventuellement manquantes : 02 pour la lettre C par exemple). On associe alors à un bloc de lettres le nombre formé en accolant les nombres associés à chaque lettre du bloc : le groupe de lettres SEMA est ainsi associé au nombre 18041200. Comme nous allons travailler modulo p, il est indispensable que les nombres ainsi obtenus soient inférieurs à p, pour éviter que deux blocs de lettres différents ne soient associés à des nombres égaux modulo p, ce qui signifie que p > 2525....25(nombre à 2m chiffres formés de m fois le nombre 25) . La fonction de codage est définie par : $f(x) \equiv x^e \pmod{p}$ et chaque nombre x associé à un bloc de lettres du message en clair est crypté par le nombre f(x) ainsi obtenu. Pour obtenir la fonction de

décodage, on utilise le petit théorème de Fermat. Comme e est premier avec p-1, il existe d tel que : $ed \equiv 1(\text{mod } p-1)$; on a alors : $[f(x)]^d \equiv [x^e]^d \equiv x^{ed}(\text{mod } p-1)$ et $ed = 1 + k(p-1)$ (puisqu'on a choisi d tel que $ed \equiv 1(\text{mod } p-1)$)donc $x^{ed} = x^{1+k(p-1)} = x^1\left(x^{p-1}\right)^k \equiv x(\text{mod } p)$ car $x^{p-1} \equiv 1(\text{mod } p)$. Ainsi la connaissance de e et p permet de calculer d, donc de retrouver x à partir de f(x).

L'exercice de l'annexe 4 explique ce procédé sur un exemple (pris dans l'article de *Repères* déjà cité). L'intérêt de cet exercice est d'être une bonne introduction au système R.S.A. : la théorie en est plus simple. D'autre part, il met en jeu des exponentiations modulo p, ce qui permet d'expliquer aux élèves la méthode d' « exponentiation rapide » .

Ce type de codage résiste à la cryptanalyse, même si on connaît des « mots probables » : on peut imaginer par exemple que le cryptanalyste sache que le nombre y=f(x) du message corresponde à un mot connu (par exemple, il peut savoir que le troisième mot du message est « secret »). Pour une valeur de x, il connaît donc à la fois x et f(x). Peut-il en déduire la clef du message ? En admettant même qu'il connaisse p, cela signifierait qu'il sait résoudre en e l'équation $x^e \equiv y(\text{mod } p)$, x , y et p étant connus. Or on ne connaît pas actuellement de méthode permettant d'éviter les essais systématiques pour e, essais dont le coût en termes de temps de calcul sur ordinateurs est élevé.

Ce type de codage est donc efficace, mais ne résout pas le problème de distribution des clés : si on veut communiquer en réseaux, la multiplication des possesseurs de clés augmente les risques de fuite. La réponse à ce problème est apportée par le concept de clé publique, inventé en 1976 par trois chercheurs américains, Diffie, Helmann et Merckle. Jusqu'au vingtième siècle, il a paru évident que le cryptage et le décryptage étaient symétriques : la même clé sert à la fois pour coder et décoder. Or les chercheurs américains pensèrent que ce n'était pas nécessaire : il suffisait de trouver une fonction arithmétique qui ne soit pas inversible ; ainsi, on pourrait rendre publique la fonction de codage, et seul, le destinataire du message pourrait décoder, grâce à une clé secrète permettant d'inverser cette fonction. L'article révolutionnaire de Diffie et Helmann présentait cependant un défaut de taille : ils étaient incapables de donner un exemple d'une telle fonction !

Diffie et Helmann proposèrent malgré tout un concept intéressant : l'échange public de clés secrètes. Nous avons souligné plus haut la difficulté de résoudre le problème de la distribution des clés. Deux personnes désirant communiquer en secret doivent échanger une clé secrète, qui est un grand nombre avec les méthodes modernes de cryptographie (comme le DES par exemple). Voici la procédure imaginée par Diffie et Helmann : on choisit un grand nombre premier q tel que $\frac{q-1}{2}$ est aussi premier, ce qui rend l'algorithme plus résistant. On choisit également un grand nombre α, de préférence racine primitive modulo q (c'est-à-dire tel que si $0 < n < q-1$ alors $\alpha^n \neq 1(\text{mod } q)$).Les nombres q et α sont publics. Le personnage A choisit secrètement un grand nombre X_A et le personnage B choisit secrètement un grand nombre X_B ; A calcule $Y_A \equiv \alpha^{X_A}(\text{mod } q)$ et B calcule $Y_B \equiv \alpha^{X_B}(\text{mod } q)$; A transmet Y_A à B et B transmet Y_B à A. La clé secrète commune est alors le nombre $K \equiv Y_B^{X_A} \equiv \left(\alpha^{X_B}\right)^{X_A} \equiv \left(\alpha^{X_A}\right)^{X_B} \equiv Y_A^{X_B}(\text{mod } q)$. La connaissance de q, α, Y_A et Y_B ne permet pas de retrouver les nombres secrets X_A et X_B, donc ne permet pas le calcul de K. La confidentialité repose sur la difficulté de calcul des « logarithmes discrets », c'est-à-dire le calcul de l'exposant d'un nombre x^n connaissant x^n et x modulo q. Mais, si cette méthode permet un échange public de clé (l'échange de Y_A et Y_B pouvant ne pas être secret), elle ne donne pas d'exemple de clé publique de cryptage.

Paradoxalement, c'est en cherchant à montrer l'impossibilité de ce concept de clef publique que Rivest, Shamir et Adleman trouvèrent une fonction convenable en 1978. Le destinataire du message (conventionnellement désigné par le prénom Alice) choisit arbitrairement deux très grands nombres premiers p et q (il existe des programmes d'ordinateurs permettant de le faire) ; il calcule le produit p.q = n et choisit un nombre e premier à (p-1)(q-1). La clef de codage est le couple (n,e) qui peut donc être rendu public. Pour coder un message, on groupe le texte en clair en blocs de m lettres, avec $n > 2525\ldots25$ (nombre de 2m chiffres). Chaque bloc est associé à un nombre (en accolant les nombres associés à chaque lettre du bloc). Ainsi le message est transformé en une suite de nombres $x_1, x_2, x_3\ldots$ tous strictement inférieurs à n. La fonction de codage est définie par : $f(x) \equiv x^e(\text{mod } n)$. Le message codé est constitué de la suite de nombres $f(x_1), f(x_2), f(x_3)\ldots$ Pour déchiffrer le message, il faut déterminer d tel que $ed \equiv 1(\text{mod}(p-1)(q-1))$ ce qui est possible car on a choisi e premier à (p-1)(q-1) ; seule Alice peut le faire car, si elle a rendu public le couple (n,e),

elle a gardé secrètes les valeurs de p et q. Le déchiffrement se fait comme ci-dessus car , si $y = f(x) \equiv x^e \pmod{n}$ alors $y^d \equiv x^{ed} \pmod{n}$ avec ed = 1 + k(p-1)(q - 1). Donc $x^{ed} \equiv x \pmod{p}$ et $x^{ed} \equiv x \pmod{q}$ et, comme p et q sont premiers entre eux, $x^{ed} \equiv x \pmod{pq}$ c'est-à-dire $x^{ed} \equiv x \pmod{n}$. On peut bien sûr utiliser également la forme généralisée par Euler du théorème de Fermat, en remarquant que, dans ce cas, $\varphi(n)=(p-1)(q-1)$, mais il est plus simple avec les élèves de raisonner directement sur p et q, en employant éventuellement le théorème de Gauss : si p divise $x^{ed} - x$ et q également, alors $x^{ed} - x = ap = bq$; donc p divise bq et, comme p est premier avec q, p divise b donc $x^{ed} - x = b'pq$ donc n = pq divise $x^{ed} - x$.

Un indiscret ne peut pas se procurer p et q, même connaissant n, car on ne connaît pas actuellement de méthode rapide permettant de factoriser de très grands nombres. La factorisation des grands nombres est un problème qui a occupé les mathématiciens bien avant l'invention de la cryptographie à clef publique et on trouvera dans ce même numéro de *Mnemosyne* un exercice d'arithmétique utilisant une lettre de Fermat à Mersenne où Fermat donne une méthode de factorisation de grands nombres[5] ; mais toutes les méthodes actuellement connues sont impuissantes à factoriser de très grands nombres (plus de 300 chiffres décimaux mais les records tombent malgré tout de temps en temps !). L'hypothèse de la difficulté de ce problème dans l'absolu sert de base à la cryptographie moderne. Cependant, on est actuellement incapable de démontrer cette hypothèse. Rien ne prouve non plus qu'il soit nécessaire de factoriser n pour « casser » le code R.S.A. : en 1998, Boneh et Verkatesan[6] ont montré qu'on peut casser le code sans factoriser n si l'exposant e est trop petit. Et, en admettant qu'un mathématicien travaillant pour des services secrets ait réussi à trouver une méthode efficace de factorisation, il ne l'a sans doute pas publiée !

A défaut de chercher une méthode de cryptanalyse de la méthode R.S.A., le lecteur intéressé pourra s'exercer au décryptage par analyse des fréquences et à la méthode de Babbage pour le système de Vigenère ; vous trouverez en effet dans les annexes 1 et 2 deux textes cryptés inventés par S. Singh qui a lancé un concours de décryptage, et, pour ces deux textes, un exemple de cryptanalyse par les méthodes exposées dans l'article. Les annexes 3 et 4 donnent le texte d'exercices donnés à des élèves de spécialité de Terminale S en 2000 sur ce thème.

---

[5] Voir également l'étude: *Factorisation de grands nombres*, page 17 dans ce numéro.

[6] D. Boneh et R. Venkatesan *Breaking RSA May Be Easier Than Factoring*, Eurocrypt 1998, LNCS 1403, Springer-Verlag.

Annexe 1 : texte à décrypter par analyse des fréquences

Extrait de *Histoire des codes secrets* de Simon Singh (Lattès 1998)

Étape 1 : Simple chiffre de substitution monoalphabétique

XT AXJ BTRJMTJ, MQQMVUVXTJ GXR NCBWJR N'UTX LMBT N'PCLLX XJ BGR XAVBDBVXTJ, XT IMAX NU AMTNXGMFVX, RUV GX QGMJVX NU LUV NU QMGMBR VCEMG. GX VCB DBJ AXJJX QMVJBX NX LMBT KUB XAVBDMBJ. MGCVR GX VCB APMTWXM NX ACUGXUV, RXR QXTRXXR G'XIIVMEXVXTJ, GXR SCBTJUVXR NX RXR VXBTR RX NXGBXVXTJ XJ RXR WXTCUZ RX PXUVJXVXTJ G'UT G'MUJVX. GX VCB AVBM MDXA ICVAX QCUV IMBVX DXTBV GXR LMWBABXTR, GXR APMGNXXTR XJ GXR MRJVCGCWUXR. GX VCB QVBJ GM QMVCGX XJ NBJ MUZ RMWXR NX FMFEGCTX : JCUJ PCLLX KUB GBVM AXJJX XAVBJUVX XJ LX IXVM ACTTMBJVX RCT XZQGBAMJBCT VXDXJBVM GM QCUVQVX, LXJJVM GX ACGGBXV N'CV M RCT ACU XJ, ACLLX JVCBRBXLX NMTR GX VCEMULX, BG ACLLMTNXVM. MGCVR DBTVXTJ JCUR GXR RMWXR NU VCB, LMBR BGR TX QUVXTJ QMR GBVX G'XAVBJUVX XJ IMBVX ACTTMBJVX MU VCB G'XZQGBAMJBCT. GX VCB FMGJPMRMV IUJ NCTA JVXR XIIVMEX, GM ACUGXUV NX RCT DBRMWX APMTWXM XJ RXR WVMTNR IUVXTJ FCUGXDXVRXR. GM VXBTX, XT VMBRCT NXR QMVCGXR NU VCB XJ NX RXR WVMTNR, DBTJ NMTR GM RMGGX NU IXRJBT. GM VXBTX QVBJ GM QMVCGX XJ NBJ : KUX GX VCB DBDX XJXVTXGGXLXTJ ! KUX JXR QXTRXXR TX J'XIIVMEXTJ QMR XJ KUX JCT DBRMWX TX APMTWX QMR NX ACUGXUV. BG E M NMTR JCT VCEMULX UT PCLLX KUB QCRRXNX XT GUB G'XRQVBJ NXR NBXUZ RMBTJR. QXTNMTJ GXR SCUVR NX JCT QXVX, UTX GULBXVX, UT NBRAXVTXLXTJ XJ UTX RMWXRRX ACLLX GM RMWXRRX NXR NBXUZ, IUVXTJ JVCUDXR XT GUB, XJ GX VCB TMFUAPCNCTCRCV JCT QXVX G'XJMFGBJ ACLLX APXI NXR NXDBTR, NXR LMWBABXTR, NXR APMGNXXTR XJ NXR MRJVCGCWUXR. QMVAX KU'UT XRQVBJ RUQXVBXUV, UTX BTJXGGBWXTAX, UT NBRAXVTXLXTJ, G'XZQGBAMJBCT NXR RCTWXR, G'BTJXVQVXJMJBCT NXR XTBWLXR, GM RCGUJBCT NXR QVCFGXLXR, IUVXTJ JVCUDXR XT GUB, XT NMTBXG, M KUB GX VCB MDMBJ NCTTX GX TCL NX FXGJRPMRRMV, KUX NMTBXG RCBJ NCTA MQQXGX XJ BG IXVM ACTTMBJVX G'XZQBAMJBCT. GX QVXLBXV LCJ RXAVXJ XRJ CJPXGGC.

Cryptanalyse du texte par analyse des fréquences

Dans les six premières lignes, voici le nombre d'apparitions de certaines lettres :
A : 7 B : 14 X : 33 G : 10 J : 13 M : 17 N : 9 T : 14 V : 14 U : 8
Il est raisonnable de penser que X est mis pour e. On considère les mots de deux lettres ; on voit fréquemment XT et XJ ; or les deux mots de deux lettres commençant par e les plus fréquents sont *en* et *et*.Essayons les deux possibilités.
Si X=e, T=t, J=n, le texte commence par : et .en .t.n.tn (les points remplaçant les lettres non encore décryptées). C'est impossible. Que donne l'autre choix ?
Si X=e, T=n, J=t, le texte commence par : en .et .n.t.nt Pourquoi pas ?
Le M très fréquent et visiblement ici mis pour une voyelle est certainement mis pour a. Continuons dans cette voie :

en .et .n.tant

Tout cruciverbiste lit alors : en cet instant
Essayons : X=e T=n J=t M=a A=c B=i R=s
en cet instant, a..a…ent .es ..i.ts .'.ne .ain .'….e et i.s ec.i.i.ent
Remettons les lettres cryptées (en majuscules pour les distinguer des lettres déchiffrées) pour bien voir apparaître les lettres doubles :
aQQaVUVent = apparurent
ecViDiVent=ecrivirent
N'Une = d'une
en cet instant apparurent Ges dCiWts d'une Lain
Et ainsi continue le décryptage maintenant facile : on a reconnu Ges=les, dCiWts=doigts Lain=main.

Annexe 2 : texte à décrypter par la méthode de Babbage

Extrait de *Histoire des codes secrets* de Simon Singh (Lattès 1998)

Étape 4 : Chiffre de Vigenère

K Q O W E F V J P U J U U N U K G L M E K J I N M W U X F Q M K J B

G W R L F N F G H U D W U U M B S V L P S N C M U E K Q C T E S W R

E E K O Y S S I W C T U A X Y O T A P X P L W P N T C G O J B G F Q

H T D W X I Z A Y G F F N S X C S E Y N C T S S P N T U J N Y T G G

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

M T F F S H N U O C Z G M R U W E Y T R G K M E E D C T V R E C F B

D J Q C U S W V B P N L G O Y L S K M T E F V J J T W W M F M W P N

M E M T M H R S P X F S S K F F S T N U O C Z G M D O E O Y E E K C

P J R G P M U R S K H F R S E I U E V G O Y C W X I Z A Y G O S A A

N Y D O E O Y J L W U N H A M E B F E L X Y V L W N O J N S I O F R

W U C C E S W K V I D G M U C G O C R U W G N M A A F F V N S I U D

E K Q H C E U C P F C M P V S U D G A V E M N Y M A M V L F M A O Y

F N T Q C U A F V F J N X K L N E I W C W O D C C U L W R I F T W G

M U S W O V M A T N Y B U H T C O C W F Y T N M G Y T Q M K B B N L

G F B T W O J F T W G N T E J K N E E D C L D H W T V B U V G F B I

J G Y Y I D G M V R D G M P L S W G J L A G O E E K J O F E K N Y N

O L R I V R W V U H E I W U U R W G M U T J C D B N K G M B I D G M

E E Y G U O T D G G Q E U J Y O T V G G B R U J Y S

Cryptanalyse par la méthode de Babbage

Il faut repérer des suites de 4 ou 5 lettres se répétant à l'identique. On remarque DOEOY répétée deux fois avec un écart de 45, NUOC avec un écart de 80. Rappelons que la longueur du mot-clef est un diviseur commun des écarts notés, donc ici de 45 et 80. Le mot-clef a donc probablement 5 lettres. Ceci est confirmé par la répétition de UU avec des écarts de 35 puis 105 lettres. Cela signifie que, si on écrit une lettre sur cinq du message, la partie du message obtenue ainsi est cryptée par un décalage unique à la mode de César. On va donc réécrire le message de façon à faire apparaître cela.

J'ai écrit les cinq premières lettres du message crypté verticalement, puis à côté les cinq suivantes et ainsi de suite. Ainsi la première ligne écrite comporte les lettres 1, 6, 11, 16, etc. du message ; la deuxième ligne comporte les lettres 2, 7, 12,etc. Nous pouvons alors appliquer l'analyse des fréquences à chaque ligne. J'ai commencé par la dernière.

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

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

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

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

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

Dans la dernière ligne, E est manifestement la lettre la plus courante. Faisons l'hypothèse qu'elle est mise pour a ou e ou i.

Si E = a, cela signifie qu'on a chiffré par un décalage de +4 et on déchiffre la dernière ligne par un décalage de –4. Alors U = q. On s'intéresse à cette lettre car les appariements possibles sont rares ; par quoi cet hypothétique q serait-il suivi ? Probablement de la lettre u sauf cas particulier. Or la lettre cryptée suivant un U de la dernière ligne est la lettre cryptée de la colonne suivante à la première ligne (vue la disposition que j'ai adoptée). Examinons différents U de la dernière ligne : ils sont suivis par des lettres différentes : J ou K ou A ; ceci n'est pas possible.

Si E = i alors on déchiffre la dernière ligne par un décalage de +4. Alors M = q. On remarque que M est suivi deux fois par W. Pourquoi pas ? Alors pour la première ligne, on a : W = u. Le déchiffrement de la première

ligne se fait par un décalage de –2. Mais alors, à la cinquième ligne, S = w est souvent suivi d'un T (de la première ligne) = r ou de N = l ou de I = g ou de S = q ou de M = k. Tout ceci est impossible.
La seule hypothèse valable pour la dernière ligne est donc E = e. La dernière ligne se déchiffre sans décalage ! La lettre Q de la dernière ligne est plusieurs fois suivie de la lettre M à la première ligne ; donc, on suppose que M = u et que la première ligne se déchiffre par décalage de +8.Essayons ; on écrit le message en déchiffrant deux lettres sur cinq et en écrivant en minuscules les lettres déchiffrées et en majuscules les autres.
sQWOenVJPurUUNusGLMesJINmeUXFquRJBge…
On peut ensuite continuer, soit avec les appariements rares, soit avec les syllabes probables. Par exemple, le premier en est peut-être suivi de t, auquel cas, dans la deuxième ligne, V = t et le déchiffrage se fait par un décalage de –2. Cela donne :
soOWentJPursUNuseLMeshINmesXFquoJBge
Le premier mot serait-il « souvent » ? Alors les lignes 3 et 4 se déchiffre par des décalages de +6 et –1. On obtient :
souventpoursamuserleshommesdequipageprennentdes
souvent pour s'amuser les hommes d'équipage prennent des.

Annexe 3: travaux pour des élèves de terminale scientifique (spécialité maths)
Exercices faits en classe

Systèmes de codages monographiques

Dans ce type de codages, chaque lettre de l'alphabet est transformée par codage en une autre lettre de l'alphabet.

Question : combien y a-t-il de permutations des lettres de l'alphabet ?

Dans la suite, chaque lettre de l'alphabet est associée à un nombre entier compris entre 0 et 25 (à l'aide de son rang dans l'alphabet). Un système de codage monographique est donc défini par une application f de $\{0,1,2,...,25\}$ dans lui-même.

Lettre	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
Nombre associé	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

EXERCICE 1 : codage par translation ; système de César

Soit x le nombre associé à une lettre de l'alphabet « en clair » et f(x) le nombre associé à la lettre « cryptée ». On considère le codage tel que :

$$f(x) \equiv x+3 (\text{mod } 26) \text{ avec } 0 \leq f(x) \leq 25.$$

1°)Coder le mot « CHOIX ».

2°)Décoder le mot « PHVVDJH ».

EXERCICE 2 : codage par transformation affine.

I)Un exemple de codage « affine ».

On considère le codage tel que f est définie par :

$$f(x) \equiv 7x+15 (\text{mod } 26) \text{ avec } 0 \leq f(x) \leq 25.$$

1°)Coder le mot « MESSAGE ».

2°)Montrer qu'il existe un unique entier relatif a' tel que :

$$7a' \equiv 1 (\text{mod } 26) \text{ et } 0 < a' < 26.$$

3°) Pour x entier de $\{0,1,2,...,25\}$, on pose : $y = f(x)$.

Montrer : $x \equiv a'.y + b' (\text{mod } 26)$ où b' est un entier relatif à déterminer..

4°) Décoder le message : « GTGRVRCSKTVPCDMR ».

II)Cas général de codage « affine ».

Soient a et b des nombres entiers relatifs. On considère le codage tel que f est définie par : $f(x) \equiv ax+b (\text{mod } 26)$ avec $0 \leq f(x) \leq 25$. Le codage est utilisable à la condition que deux lettres différentes soient codées différemment.

1°)On suppose : a est premier avec 26.

Montrer qu'alors : $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

2°)On suppose : PGCD(a, 26)=d avec d > 1. On a alors : 26 = d.k avec 0 < k < 26.

Montrer que, dans ce cas, $f(k) = f(0)$.

Dans la suite de l'exercice, a est premier à 26.

3°)Fonction de décodage.

a)Montrer qu'il existe a' entier relatif tel que $a.a' \equiv 1 (\text{mod } 26)$.

b)Pour x entier de $\{0,1,2,...,25\}$, on pose : $y = f(x)$.

Montrer : $x \equiv a'.y + b' (\text{mod } 26)$ où b' est un entier relatif à déterminer.

Annexe 4 : travaux pour des élèves de terminale scientifique (spécialité maths)
Devoir à la maison(annexe faite en travaux dirigés en classe)

Dans les deux exercices suivants, on utilisera le « petit théorème de Fermat » :
Soit p un nombre premier et a un entier relatif premier à p , alors : $a^{p-1} \equiv 1 (\text{mod } p)$.

Comme pour les codages monographiques, chaque lettre de l'alphabet en « clair » est associée à un « équivalent numérique », mais qui a obligatoirement deux chiffres, éventuellement en ajoutant un zéro devant le rang de la lettre.

Lettre	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
Nombre associé	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Pour éviter le déchiffrement par analyse statistique, on groupe le message en blocs de m lettres, ce qui donne un nombre de 2m chiffres (en comptant les éventuels zéros en tête de l'écriture). Le codage consiste alors à déterminer une fonction arithmétique f que seul le destinataire du message peut inverser. Les exercices suivants propose deux types de codage actuellement utilisés.

Exercice 1 : codage par exponentiation.

Soit p un nombre premier. Nous allons travailler « modulo p » ; il est donc nécessaire que deux nombres de 2m chiffres obtenus par regroupement en blocs de m lettres d'un message initial soit toujours différents modulo p ; on choisira m le plus grand possible (pour rendre le déchiffrement moins aisé) tel que le plus grand nombre obtenu par regroupement de m lettres soit inférieur strictement à p. Pour m =2 par exemple, le plus grand nombre possible ainsi obtenu est 2525 et on ne pourra faire des blocs de deux lettres que si p>2525.

1°) Compléter le tableau suivant :

Entier premier p choisi	Plus grand entier m convenable
25 <p < 2525	m= 1
2525 < p <	m= 2
	m=
	m=

Remarque : ce tableau est infini.

Pour éviter un décodage facile par analyse des fréquences, il faut donc que p soit un très grand nombre premier.

Dans la suite de l'exercice, e désigne un entier naturel premier à p-1.

Soit x un nombre entier tel que : $0 \le x \le p-1$. On définit la fonction arithmétique f par : $f(x) \equiv x^e (\text{mod } p)$ avec $0 \le f(x) \le p-1$. Le codage consiste à remplacer chaque bloc de m lettres par le nombre f(x) correspondant. Le couple (p, e) constitue la clef de codage.

2°)Calcul de x^e modulo p pour e et p donnés.

Nous avons vu en exercice comment calculer x^n modulo p pour n'importe quel entier naturel n. Ce calcul est simple à effectuer lorsque p est petit ; mais, lorsque p est grand, ce qui est toujours le cas dans les problèmes de codage, il faut trouver un moyen de réduire le temps de calcul : comment calculer effectivement, par exemple, $251^{35} (\text{mod } 1987)$ avec des opérations qui ne dépassent pas les capacités de la calculatrice et qui ne prennent pas trop de temps ? Une méthode efficace est la suivante :

*on décompose 35 en somme de puissances de 2 : $35 = 2^5 + 2 + 1$.

*on calcule 251^{2^n} modulo 1987 pour n=0 à 5 par élévations au carré successives de la manière suivante :

$$251 \equiv 251 (\text{mod}\, 1987)$$
$$251^2 \equiv 1404 (\text{mod}\, 1987)$$
$$251^{2^2} = \left(251^2\right)^2 \equiv 1404^2 \equiv 112 (\text{mod}\, 1987)$$
$$251^{2^3} = \left(251^{2^2}\right)^2 \equiv 112^2 \equiv 622 (\text{mod}\, 1987)$$
$$251^{2^4} = \left(251^{2^3}\right)^2 \equiv 622^2 \equiv 1406 (\text{mod}\, 1987)$$
$$251^{2^5} = \left(251^{2^4}\right)^2 \equiv 1406^2 \equiv 1758 (\text{mod}\, 1987)$$

*on calcule enfin $251^{35} (\text{mod}\, 1987)$:

$$251^{35} = 251^{2^5} \times 251^2 \times 251 \equiv 1758 \times 1404 \times 251 (\text{mod}\, 1987)$$
$$\equiv 378 \times 251 \equiv 1489 (\text{mod}\, 1987)$$

Nous avons effectué en tout 5 élévations au carré et 2 multiplications modulo 1987 ; nous sommes loin des 34 multiplications nécessaires pour élever à la puissance 35 .

Pour voir si vous avez compris, expliquez comment calculer 304^{29} modulo2633 et faites les calculs intermédiaires avec votre calculatrice. Les calculatrices disposent en général d'une fonction donnant directement le reste de la division euclidienne d'un nombre a par un nombre b(par exemple, dans la TI80, on trouve dans le menu MATH NUM la fonction REMAINDER ; REMAINDER(304^2,2633) vous donne le reste de la division euclidienne de 304^2 par 2633,i.e.261).

3°)Codage d'un message.

Dans cette question, p=2633 et e=29.

a)Comment faudrait-il procéder pour vérifier que p est premier à l'aide de la table de nombres premiers de votre livre de spécialité (donner les explications sans faire les calculs) ?

b)Vérifier que 2632 et 29 sont premiers entre eux.

c)Quelle est la valeur de m correspondant à p ? p est-il suffisamment grand pour éviter un décodage par analyse des fréquences ?

d)Coder le message : « CODE SECRET ».Pour cela :

*Ecrire le message groupé en blocs de m lettres sans tenir compte de l'espace et, sous le message ainsi écrit, noter l'équivalent numérique de chaque bloc.

*Elever chaque nombre correspondant à un bloc à la puissance 29 modulo 2633.

L'élévation à la puissance 29 modulo 2633 est suffisamment fastidieuse pour mériter un traitement informatique. Voir annexe avant de faire les calculs.

4°)Décoder un message. Dans cette question, p=2633 et e=29.

a)Montrer qu'il existe un entier relatif u tel que : $29u \equiv 1(\text{mod}(2632))$. En déduire qu'il existe un unique entier naturel d tel que : $29d \equiv 1(\text{mod}(2632))$ avec $0 \le d < 2632$ et calculer d.

b)En déduire : $f(x)^d \equiv x (\text{mod}\, 2633)$. La fonction de décodage est donc définie par : $g(y) \equiv y^d (\text{mod}\, 2633)$ avec $0 \le g(y) < 2633$.

b)Décoder le message :

0500	1868	0951	0815	2165	0680	1130

Pour cela, il faut élever chaque nombre du tableau à la puissance d modulo 2633. Expliquer la marche à suivre et utiliser Excel pour le faire.

5°)Cas général.

On rappelle que p est un nombre premier quelconque et que e est un nombre entier positif premier avec p-1.

a)Montrer qu'il existe un entier relatif u tel que : $e.u \equiv 1(\text{mod}(p-1))$. En déduire qu'il existe un unique entier naturel d tel que : $e.d \equiv 1(\text{mod}(p-1))$ avec $0 \le d < p-1$.

b)En déduire : $f(x)^d \equiv x(\text{mod}\, p)$. La fonction de décodage est donc définie par : $g(y) \equiv y^d (\text{mod}\, p)$ avec $0 \le g(y) < p$.

Ce type de codage résiste bien à la cryptanalyse si p est suffisamment grand. Cependant, si les messages doivent circuler sur un réseau, un nombre important de personnes doivent connaître les clés de codage, ce qui augmente les risques de fuite. L'exercice 2 présente un moyen d'éliminer ce défaut.

Exercice 2 : codage à clés publiques ; système R.S.A.

La clé de codage est un couple d'entiers naturels (e,n) rendu public.

On a : n = p.q où p et q sont des nombres premiers distincts et très grands. La décomposition de n en facteurs premiers n'est connue que de la personne destinataire du message. Le nombre e est premier avec (p-1)(q-1).

Pour coder le message, on découpe le texte en blocs de m lettres, chaque bloc ayant un équivalent numérique comme dans l'exercice 1. Nous allons travailler modulo n, d'où une condition sur m en fonction de n.

Si x est l'équivalent numérique d'un bloc, la fonction de codage est définie par : $f(x) \equiv x^e (\mathrm{mod}\, n)$ avec $0 \leq f(x) < n$.

1°)Montrer qu'il existe un unique entier naturel d tel que : $e.d \equiv 1 (\mathrm{mod}(p-1)(q-1))$ avec $0 \leq d < (p-1)(q-1)$.

2°)a)Montrer : $x^{ed} \equiv x (\mathrm{mod}\, p)$ et $x^{ed} \equiv x (\mathrm{mod}\, q)$.

b)En déduire : $x^{ed} \equiv x (\mathrm{mod}\, n)$.

3°)Quelle est la fonction de décodage ?

Annexe au problème(aidant à traiter la question 3°) de l'exercice 1)

1°)Ecrire un algorithme permettant à une calculatrice programmable de calculer N^{29} modulo 2633 pour N quelconque. L'algorithme commence par : $? \rightarrow N$ afin de pouvoir entrer n'importe quelle valeur pour N ; utiliser la fonction REMAINDER pour simplifier l'écriture de l'algorithme.

2°)Voici enfin l'occasion d'apprendre à se servir d'un tableur !

Tous les ordinateurs du lycée disposent d'un tableur[7], capable d'exécuter des calculs comme une calculatrice programmable. Nous allons nous en servir pour calculer 304^{29} modulo 2633. Voici la marche à suivre intelligemment, c'est-à-dire en essayant de comprendre ce qui se passe :

Ouvrir une feuille de calcul ; on voit apparaître un tableau à double entrée dont chaque case s'appelle une « cellule ». Pour sélectionner une cellule, on clique dessus ; pour sélectionner un groupe de cellules, on clique sur la première du groupe et, en maintenant le bouton de la souris enfoncé, on glisse jusqu'à la dernière où on relâche le bouton. Les cellules sélectionnées sont en surbrillance.

Commençons par indiquer sur la feuille de calculs ce que nous calculons :

Sélectionner la cellule A1 puis taper [n] puis [entrée].

Sélectionner la cellule B1 puis taper [a^(2^n)mod2633] puis [entrée].

Maintenant, nous allons programmer les calculs. Il est nécessaire pour comprendre d'avoir traité la question 2°) de l'exercice 1.

Sélectionner la cellule A2 puis taper 0 puis [entrée].

Sélectionner la cellule A3puis taper [=A2+1] (pour taper A2 dans cette formule, cliquer sur la cellule A2), puis taper [entrée].

Sélectionner les cellules A3 jusqu'à A6, puis cliquer sur [Edition] et, en maintenant le bouton de la souris enfoncé, glisser jusqu'à [recopier], puis dans le sous-menu qui s'ouvre alors, glisser jusqu'à [en-bas] et relâcher le bouton de la souris. Examiner ce qui se passe.

Sélectionner B2 ; taper 304 puis [entrée].

Sélectionner B3 ; taper [=] ; dans le menu [Insertion], choisir [Fonction] puis [math&trigo] et [MOD] ; lire les indications données et mettre dans B3 [=MOD(B2^2,2633)] puis [entrée].

Sélectionner les cellules B3 à B6 et recopier vers le bas.

Avec la même procédure, mettre dans C2 [=MOD(B2*B4,2633)] et dans C3 [=MOD(B5*B6,2633).]

Que faut-il mettre dans C6 pour obtenir le résultat final, c'est-à-dire 304^{29} modulo 2633 ?

Si on remplace 304 par 1502, qu'obtient-on ?

---

[7] Cette annexe a été établie pour des élèves du lycée Flora Tristan(93 – Noisy-le-Grand), alors que nous disposions du tableur Excel. Les instructions peuvent différer légèrement pour un autre tableur(Lotus par exemple).

Annexe 5 : articles du *Monde*.

Un nouvel algorithme de cryptage belge s'impose aux Etats-Unis

Cette victoire improbable a réjoui les spécialistes européens de la cryptographie, cette « science du secret » qui consiste à coder et décoder efficacement des données. Au terme d'une compétition internationale qui a duré trois ans, le département du commerce américain a choisi, lundi 2 octobre, un algorithme de cryptage belge, baptisé Rijndael, pour succéder au DES (Data Encryption Standard).

...

Contrairement au DES, qui avait été développé en grand secret par IBM,l'AES a été choisi au terme d'une procédure transparente particulièrement sévère.

Le Monde octobre 2000

www.cryptonline.com

Crypter n'importe quel document, gratuitement, rapidement et sans formalité

...Le service, baptisé « Cryptonline »est gratuit, automatique, ouvert à tous, et ne prend que quelques secondes....Cryptonline utilise un cryptage à 56 bits, c'est-à-dire de moyenne puissance, faisant appel à des algorithmes standard....Cryptonline n'est donc pas fait pour protéger les secrets d'Etat

Le Monde 18 janvier 2001

Bibliographie

Simon SINGH *Histoire des codes secrets* Ed . J.C.Lattès paris 1999

Jacques STERN *La science du secret* Ed. Odile Jacob Paris 1998

Jean-Paul DELAHAYE *Merveilleux nombres premiers* Ed. Belin-Pour la Science Paris 2000

Robert NOIRFALISE *Arithmétique et cryptographie* in *Repères* n°37 octobre 1999 (pages 41-62)

Martin HELMANN *Les mathématiques de la cryptographie à clef révélée* in *Pour la Science 1979*

Jean-Paul DELAHAYE *La cryptographie RSA vingt ans après* in *Pour la Science* n° 267 Janvier 2000

MATHEMATIQUES ET THEATRE

Anne Michel-Pajus
(Traduction et commentaires)

Breaking the code

Hugh Whitemore, Samuel French Ltd, 1987,1988

Il s'agit d'une pièce écrite d'après le livre *Alan Turing, The Enigma*, d'Andrew Georges.
Elle a été représentée en France durant l'hiver 2000 (nous n'en connaissons pas de traduction française).

Alan Turing

Quatrième de couverture

"Une pièce empathique et souvent amusante sur l'esprit remarquable et le tragique destin d'Alan Turing, mathématicien et pionnier de l'informatique, qui brisa le code de deux façons. L'une en cassant le code de l'Enigma allemande à Bletchley Park pendant la deuxième guerre mondiale, ce pour quoi il fut décoré par Churchill et loué par la nation ; la seconde en brisant le code de discrétion sexuelle du gentleman anglais par son manque d'efforts pour cacher son homosexualité, ce pour quoi il fut arrêté sous la charge d'indécence grave. La pièce de Whitemore, construite en aller-retours dans le temps, cherche constamment une connexion entre les deux événements et aborde des questions majeures comme la relation entre les mathématiques et la morale personnelle, tout en racontant une excellente histoire."

Nous reproduisons ci-dessous quelques extraits de la pièce ayant trait à l'Enigma.

Extrait de l'Acte I, scène 6 (pp.18-19)

[Turing arrive à Bletchley Park, le siège des Services Britanniques de Décodage, pendant la seconde guerre mondiale.]

" **Knox** : Le problème, c'est que ce foutu code est une part vitale de l'effort de guerre nazi – vitale. L'armée l'utilise, la Luftwaffe aussi, et – surtout – les sous-marins. Et si les sous-marins prennent le contrôle de l'Atlantique Nord, notre flotte marchande n'a pas l'ombre d'une chance. Ils vont nous faire crever de faim. Donc – il faut casser l'Enigma. Top Priorité.

Turing : De quel type de code s'agit-il ?

Knox rassemble ses documents éparpillés et les remet dans le dossier.

Pat : Mécanique.

Knox : Ce qui met la balle clairement dans votre camp.[...]

Knox sort.

Pat se dirige vers la porte après lui.

Pat : Je vous verrai lundi.

Turing : Attendez , hum – pouvez-vous me dire – en quel sens l'Enigma est-elle mécanique ?

Pat : Eh bien, le code est créé par une machine. Ça ressemble un peu à une machine à écrire ; il y a trois rotors derrière le clavier, avec les lettres de l'alphabet autour de chaque rotor, et derrière les rotors, un tableau d'affichage. Si l'opérateur appuie sur une touche – disons la lettre « A » – avec les rotors dans une position donnée, une connexion se fait avec, par exemple, la lettre « D » et une lampe s'allume sur le tableau à la lettre « D ».

Turing : Le texte « A » est encodé en « D ».

Pat : Oui, avec les rotors dans cette position déterminée. Ensuite, le premier rotor bouge. Appuyer sur « A » peut maintenant donner un « P » ou un « H » sur le tableau. Quand le rotor a fait un tour complet, le deuxième fait de même, puis le troisième. C'est une machine polyalphabétique avec vingt-six fois [vingt-six fois] vingt-six positions.

Turing : Dix-sept mille cinq cent soixante seize. Ce n'est pas un nombre terriblement grand.

Pat : Non, c'est exact. Une analyse à la main finirait pas conduire à la position correcte, avec un peu de patience, mais cela pourrait prendre plusieurs jours, et la position est changée tous les jours. Les Allemands utilisent un carnet de codes pour indiquer la position – nous ne l'avons pas, évidemment – mais au moins , nous savons maintenant comment ça marche – et on a réussi à construire une machine qui simule la fonction de l'Enigma, qui est logique, symétrique et involutive.

Turing : L'expéditeur et le receveur ont le même équipement.

Pat : Oui. L'ennui c'est que les Allemands viennent de rendre l'Enigma beaucoup plus sophistiquée, ce qui signifie que notre machine est virtuellement obsolète. Leurs opérateurs sont maintenant équipés d'une réserve de cinq rotors parmi lesquels n'importe quel groupe de trois peut être utilisé, dans n'importe quel ordre, quand ils branchent l'Enigma.

Turing : Soixante combinaisons possibles ! Dix-sept mille cinq cent soixante seize fois soixante !

Pat : Un million cinquante quatre mille cinq cent soixante. Ils ont aussi ajouté un tableau de branchements à l'appareil – comme un standard téléphonique. Ils connectent des paires de lettres avec des fiches et ceci échange les lettres avant qu'elles ne soient entrées dans les rotors – et après. Il y a ainsi littéralement des milliers de millions de permutations possibles ; et c'est le problème que nous devons résoudre – le problème de base en tout cas ; l'Enigma utilisée dans les sous-marins est encore plus compliquée. (*Une grimace*) Bien, on se voit lundi."

Extrait de l'Acte II, scène 6 (p.55)

[Les Services Secrets craignent que l'homosexualité de Turing ne le conduise à trahir involontairement des secrets et le soumettent à une étroite surveillance.]

"**Turing** : Je veux que vous sachiez que je n'ai aucun regret de mon implication dans les Services Secrets. Le travail que j'ai fait à Bletchley était très important pour moi.

Smith : Oui, j'en suis certain.

Turing : Important en un sens que vous ne pouvez sans doute pas comprendre. Ça a demandé plus que des mathématiques et de l'électronique pour casser l'Enigma des sous-marins. Il a fallu de la détermination, de la ténacité – de la fibre morale, si vous voulez. Voilà ce qui l'a rendu si profondément gratifiant. Tout se tenait ensemble. Tous les fils de ma vie. Mon travail de mathématicien. Mon intérêt pour les chiffres. Ma capacité à résoudre les problèmes pratiques. L'amour de mon pays. Pendant une année à peu près, j'ai senti que j'avais trouvé ce que je cherchais. Vous me faisiez confiance, alors. Pourquoi pas maintenant ?"

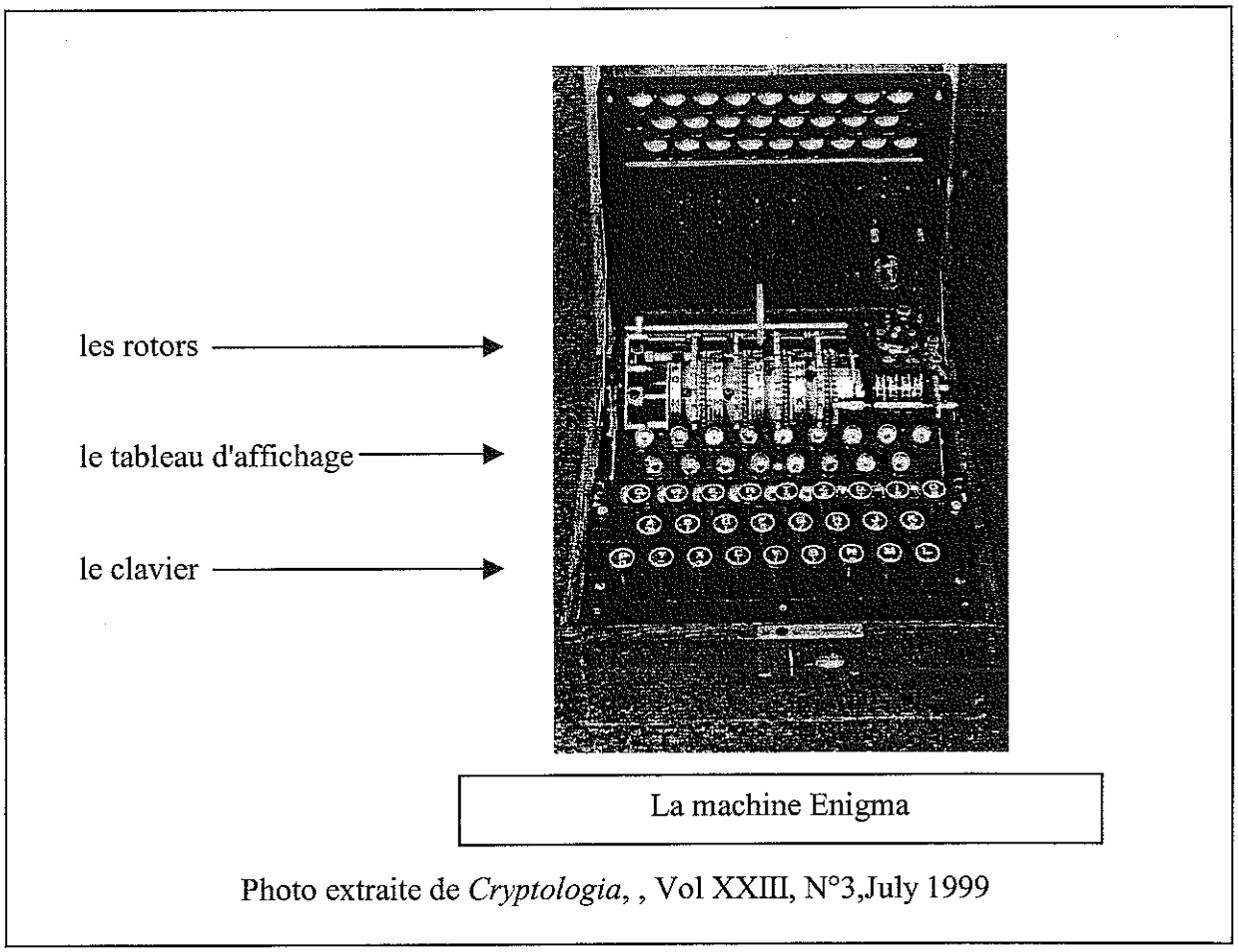
Extrait de Acte II, scène 7 (pp.57-58)

[Lors de vacances à Corfou, Turing répare le poste de radio d'un amant grec, Nikos, qui ne comprend pas l'anglais.]

" Nikos embrasse Turing, qui est à la fois ému et embarrassé.

Turing : Merci, mon cher Nikos ? Merci. *(Il sourit*) On se sent bien, n'est-ce-pas ? Résoudre un problème, trouver la réponse. Faire marcher. On se sent bien. C'est comme cette TSF, vraiment ; toute la question est de faire les bons branchements. (*Une courte pause ; une idée se glisse dans son esprit*) Vous confierai-je un secret ? Top secret. Je ne pourrais pas en parler à mon analyste. Mais puisque vous n'y comprendrez pas un traître mot, ça n'a pas vraiment d'importance. Tout cela remonte au début de la guerre dans une maison de campagne anglaise appelée Bletchley Park. Les Allemands avaient construit une machine appelée Enigma. C'était très astucieux. Elle fabriquait des codes – personne ne savait comment casser les codes qu'elle fabriquait. Voilà le problème qu'il nous fallait résoudre. Si on ne l'avait pas fait, si on n'y était pas arrivé, on aurait perdu la guerre – c'était aussi simple que ça. Mais par où commencer ? Et bien, d'abord, c'était une devinette. Le processus de déchiffrage du code commençait toujours par une devinette. Il fallait deviner ce que les premières phrases du message pouvaient signifier. Ce n'était pas si difficile que ça en a l'air parce que les messages militaires commencent invariablement par une phrase stéréotypée : la date, l'heure, le nom et le grade de l'expéditeur, ce genre de choses. Ensuite, nous découvrîmes qu'il était possible d'utiliser la phrase que nous avions devinée pour former une chaîne d'implications, de déductions logiques, pour chacune des positions des rotors. Si cette chaîne d'implications conduisait à une contradiction – ce qui était généralement le cas – ça signifiait qu'on s'était trompé, et il fallait essayer la position suivante du rotor. Et ainsi de suite et ainsi de suite. Un processus impossiblement long et laborieux. On avait le temps contre nous ; on ne savait que faire. Alors, tout à coup, un après-midi de printemps, je me suis souvenu d'une conversation avec Wittgenstein ; on discutait du fait qu'une contradiction peut conduire à n'importe quelle proposition – et je vis – immédiatement – que je pourrais utiliser ce théorème élémentaire de logique mathématique pour construire une machine qui aurait la vitesse nécessaire : une machine avec des relais électriques et des circuits logiques qui sentirait les contradictions

et reconnaîtrait les consistances, une machine de boucles fermées et de parfait synchronisme, une machine à distinguer un motif dans l'absence de motifs. Si vous aviez mal deviné, l'électricité affluerait dans toutes les hypothèses en corrélation et les ferait exploser en un éclair – comme la réaction en chaîne d'une bombe atomique. Si votre hypothèse était correcte, tout serait consistant, – et le courant électrique s'arrêterait à la combinaison correcte. Notre machine pourrait examiner des milliers de millions de possibilités à une vitesse stupéfiante, et avec un peu de chance, nous donnerait la « voie d'accès ». Plus que cela : toutes les connections avaient été faites. C'était la beauté pure du schéma logique. L'élément humain. La relation profondément gratifiante entre le théorique et le pratique. Quel moment ce fut. Absolument, absolument extraordinaire. (*Pause*) Oh, Christopher … Si seulement tu avais été là. Plus jamais. Plus jamais un moment comme ça. (*Pause*) Au bout du compte, ce n'est pas de casser le code qui compte – c'est où l'on va ensuite. C'est ça le vrai problème."



La machine Enigma

Photo extraite de *Cryptologia*, , Vol XXIII, N°3,July 1999

La personnalité d'Alan Turing et la machine Enigma ont suscité de nombreuses œuvres plus ou moins de fiction. Parmi celles-ci, citons :

Jean Lassègue, *Turing*, Les Belles Lettres, 1998

(une biographie philosophique)

Gérard Ramstein *Requiem pour une puce*, Seuil

(roman policier dont les protagonistes sont baptisés de noms de mathématiciens et dans lequel on retrouve les idées qui ont donné naissance à l'informatique)

Robert Harris, *Enigma*, Pocket 1997

(une fiction policière qui se déroule à Bletchley Park durant la deuxième guerre mondiale)

DANS NOS CLASSES

Thèmes abordés : arithmétique
Niveau : Terminale S
Outils nécessaires : nombres premiers puis, pour un prolongement en classe, congruences
Texte étudié : une lettre de Fermat à Mersenne (1643)

Martine Bühler

Le problème des pages suivantes est l'aboutissement d'un travail effectué en 2000 avec des participants à un stage d'histoire des mathématiques à l'I.R.E.M. Paris VII ; il a été donné en devoir à la maison à des élèves de terminale scientifique, spécialité mathématiques. Il permet d'aborder le thème de la factorisation des grands nombres[1] à partir d'une lettre de Fermat à Mersenne de 1643.

La première partie du problème est assez aisée ; cependant, la deuxième partie, qui s'attaque à un algorithme de factorisation indiqué par Fermat, a semblé difficile aux élèves et a nécessité une correction soignée en classe. La troisième partie traite de longueur d'algorithme et introduit un début de réflexion sur les nombres carrés, qui s'appuie sur une remarque de Fermat. Lors de la correction en classe, nous avons travaillé sur les congruences pour reconnaître si un nombre peut être un carré ou non, puis nous avons visionné un film sur la machine à congruences des frères Carissan[1].

[1] Voir l'étude *Factorisation de grands nombres* dans ce mêmes numéro, page 17

Devoir à la maison donné en Terminale S (spécialité maths)

En 1643, Fermat répond à Mersenne qui lui a lancé le défi de factoriser 100 895 598 169. Il trouve cette factorisation (898 423 x 112 303), mais indique dans une lettre ultérieure une méthode générale. C'est cette lettre que nous allons lire ensemble.

I.DIFFERENCE DE DEUX CARRES ET FACTORISATION

Soit N un nombre entier naturel impair.

1°) On suppose que $N=a^2-b^2$ avec a et b entiers naturels. Déterminer deux entiers naturels p et q tels que N=pq.

2°) On suppose que N=pq avec p et q entiers naturels et p > q.

a) Quelle est la parité de p et q ?

b) Montrer qu'il existe deux entiers naturels a et b tels que $N=a^2-b^2$.

c) Démontrer que :

« p et q sont premiers entre eux » équivaut à « a et b sont premiers entre eux ».

3°) Fermat utilise les définitions suivantes :

Les nombres compositeurs sont les facteurs d'un nombre composé.

Ex : 45 = 9x5 ; 9 et 5 sont les compositeurs du nombre composé 45.

Les parties d'un nombre sont ses diviseurs, c'est-à-dire les compositeurs.

a) Lire le texte lignes 1 à 14 (attention, à la ligne 2, traduire « *ou* » par « *c'est-à-dire* »).

b) Quelle est la phrase du texte de Fermat correspondant aux questions 1°) et 2°)b) ?

c) Quelle est la phrase du texte de Fermat correspondant à la question 2°)c) ?

d) Que se passe-t-il si N est un carré ?

e) Lire les lignes 15 et 16 et les traduire avec des notations algébriques.

II.ALGORITHME DE FACTORISATION

1°) Quelles sont les questions que pose Fermat dans les lignes 20-21-22 ?

Dans la suite on pose N = 2 027 651 281.

2°) Pour résoudre son problème, Fermat cherche deux nombres a et b tel que a^2-N est un carré.

a) Pourquoi ?

b) Quelle est la valeur minimale de a pour que a^2-N soit un carré ?

c) Si vous savez utiliser un tableur, rechercher à l'aide du tableur le plus petit entier a solution du problème ; vous joindrez à la copie la feuille de calcul du tableur et un tableau indiquant comment vous avez rempli les cellules.

d) Ecrire un algorithme permettant de programmer votre calculatrice pour obtenir la plus petite solution a. Donner a.

3°) Fermat, ne disposant pas d'un ordinateur, faisait ses calculs à la main et a préféré, avant de calculer, améliorer l'algorithme ; il emploie donc une procédure de calcul équivalente à la vôtre, mais évitant les élévations au carré. Le but de cette question est de comprendre son algorithme.

Dans la suite $X_0=E(\sqrt{N})$ (partie entière de $\sqrt{N}$)= 45 029, R=40 440 et $A_0=X_0+1$.

a) Lire les lignes 23-24(jusqu'à « de reste ») et écrire une égalité liant N, X_0 et R.

b) Pourquoi s'intéresse-t-on à A_0 ?

c) On pose : $U_0=2X_0+1$ et $B_0=U_0-R$. Sans utiliser les valeurs numériques, montrer que $B_0 = A_0^2 - N$.

La question est donc de savoir si B_0 est un carré. Calculer les valeurs numériques de U_0 et B_0 répondre à la question ; lire les lignes 23 à26 jusqu'à « ne finit par 19 ».

4°) On pose, pour p entier naturel, $A_{p+1} = A_p + 1$; $U_{p+1} = U_p + 2$; $B_{p+1} = B_p + U_{p+1}$.

a) Vérifier, sans utiliser les valeurs numériques, que $A_1^2 - N = B_1$.

Quelle question se pose-t-on sur B_1 ? Calculer B_1 et répondre à la question.

b) Montrer : pour p entier naturel, $U_{p+1} = 2 A_p + 1$ et $A_p^2 - N = B_p$.

Lire les lignes 26 à 36.

5°) a) A quel moment Fermat arrête-t-il ses calculs ?

b) Pour p entier naturel, exprimer A_p à l'aide de X_0 et p, et exprimer p à l'aide de U_p et U_1.

c) Quelle est la valeur numérique B_{p_0} à laquelle Fermat arrête ses calculs ? Quelle est la valeur numérique U_{p_0} correspondante (voir les lignes 37 à 39) ? Calculer p_0, puis A_{p_0}.

d) Exprimer N comme différence de deux carrés, puis comme un produit de facteurs.

e) Lire la fin du texte.

III. COMPLEMENTS

1°) Utiliser un tableur pour programmer l'algorithme de Fermat.

2°) Ecrire un algorithme permettant de programmer votre calculatrice pour effectuer les calculs de Fermat.

3°) Expliquer les phrases suivantes du texte :

« reste 49 619, lequel n'est pas quarré, parce que aucun quarré ne finit par 19 ».

« car les carrés ne peuvent souffrir les finales qu'elles ont ».

4°) Lorsque $N = a^2 - b^2$,quel est le nombre d'étapes nécessaires dans l'algorithme de Fermat pour trouver a ?

Quel est le nombre d'étapes nécessaires pour factoriser 100 895 598 169 ? Qu'en pensez-vous ?

5°) Si N est premier, la seule factorisation possible de N est N = N x 1. Quelle est alors la valeur correspondante de a ? Quel est le nombre d'étapes nécessaires dans l'algorithme de Fermat pour aboutir ? L'algorithme de Fermat peut ainsi servir de test de primalité ; je l'appellerai « test historique » bien que ni Fermat, ni ses successeurs ne l'aient utilisé comme test de primalité. Ce « test historique » est-il plus efficace que votre « test habituel » ?

Extrait des *Œuvres*, éd. Tannery et Henry, tome II, 1894, Lettre de 1643, pp. 257-258.

LVII.

FRAGMENT D'UNE LETTRE DE FERMAT (²).

< 1643 >

(A, f° 74.)

Tout nombre impair non quarré est différent d'un quarré par un quarré, ou est la différence de deux quarrés, autant de fois qu'il est composé de deux nombres, et, si les quarrés sont premiers entre eux, les nombres compositeurs le sont aussi. Mais si les quarrés ont entre eux un commun diviseur, le nombre en question sera aussi divisible par le même commun diviseur, et les nombres compositeurs seront divisibles par le côté de ce commun diviseur.

Par exemple : 45 est composé de 5 et de 9, de 3 et de 15, de 1 et de 45. Partant, il sera trois fois la différence de deux quarrés : savoir de 4 et de 49, qui sont premiers entre eux, comme aussi sont les compositeurs correspondants 5 et 9; plus, de 36 et de 81, qui ont 9 pour commun diviseur, et les compositeurs correspondants, 3 et 15, ont le côté de 9, savoir 3, pour commun diviseur; enfin 45 est la différence de 484 et 529, qui ont 1 et 45 pour compositeurs correspondants.

Il est fort aisé de trouver les quarrés satisfaisants, quand on a le nombre et ses parties, et d'avoir les parties lorsqu'on a les quarrés.

Cette proposition se trouve quasi tout par tout. On en pourrait quasi autant dire des pairements pairs, excepté 4, avec quelque petite modification.

Cela posé, qu'un nombre me soit donné, par exemple 2 027 651 281, on demande s'il est premier ou composé, et de quels nombres il est composé, au cas qu'il le soit.

J'extrais la racine, pour connoître le moindre des dits nombres, et trouve 45 029 avec 40 440 de reste, lequel j'ôte du double plus 1 de la racine trouvée, savoir de 90 059 : reste 49 619, lequel n'est pas quarré, parce que aucun quarré ne finit par 19, et partant je lui ajoute 90 061, savoir 2 plus que 90 059 qui est le double plus 1 de la racine 45 029. Et parce que la somme 139 680 n'est pas encore quarrée, comme on le voit par les finales, je lui ajoute encore le même nombre augmenté de 2, savoir 90 063, et je continue ainsi d'ajouter tant que la somme soit un quarré, comme on peut voir ici (¹). Ce qui n'arrive qu'à 1 040 400, qui est quarré de 1020, et partant le nombre donné est composé; car il est aisé, par l'inspection des dites sommes, de voir qu'il n'y a aucune qui soit nombre quarré que la dernière, car les quarrés ne peuvent souffrir les finales qu'elles ont, si ce n'est 499 944 qui néanmoins n'est pas quarré.

Pour savoir maintenant les nombres qui composent 2 027 651 281, j'ôte le nombre que j'ai premièrement ajouté, savoir 90 061, du dernier ajouté 90 081. Il reste 20, à la moitié duquel plus 2, savoir à 12, j'ajoute la racine premièrement trouvée 45 029. La somme est 45 041, auquel nombre ajoutant et ôtant 1020, racine de la dernière somme 1 040 400, on aura 46 061 et 44 021, qui sont les deux nombres plus prochains qui composent 2 027 651 281. Ce sont aussi les seuls, pource que l'un et l'autre sont premiers.

Si l'on alloit par la voie ordinaire, pour trouver la composition d'un tel nombre, au lieu de onze additions, il eût fallu diviser par tous les nombres depuis 7 jusqu'à 44 021.

Plusieurs abrégés se peuvent trouver, comme lorsqu'on ne fait qu'une addition au lieu de dix, aux endroits où les sommes ont leurs finales quarrées, quand les compositeurs sont beaucoup éloignés l'un de l'autre.

LVI.

FERMAT A MERSENNE (1).

MARDI 7 AVRIL 1643.

(A, f^os 19-20; B, f° 22 v°.)

4. Vous me demandiez donc quelle proportion a le nombre, qui se produit des nombres suivants, avec ses parties aliquotes :

214 748 364 800 000, 11, 19, 43, 61, 83, 169, 223, 331, 379, 601, 757, 961, 1201, 7019, 823 543, 616 318 177, 6561, 100 895 598 169.

Vous me demandiez ensuite si ce dernier nombre est premier ou non, et une méthode pour découvrir dans l'espace d'un jour s'il est premier ou composé.

A la première question, je vous réponds que le nombre qui se fait de tous les nombres précédents multipliés entre eux, est sous-quintuple de ses parties.

A la seconde question, je vous réponds que le dernier de ces nombres est composé et se fait du produit de ces deux :

$$898\,423 \quad \text{et} \quad 112\,303^3,$$

qui sont premiers (1).

Je suis toujours, mon Révérend Père,

Votre très humble et très affectionné serviteur,

FERMAT.

A Toulouse, ce 7 avril 1643.

Paris chez Petit rue S. Jacques pres les Mathurins

NOTES DE LECTURE

Anne Michel-Pajus

Mathématiques et physique leibniziennes *Revue d'histoire des sciences*, Tome 54-2-Avril-Juin 2001, PUF.

La revue consacre deux parutions à Leibniz. Celle de juin 2001 est consacrée aux mathématiques, celle de Septembre 2001, que je n'ai pas lue, est davantage tournée vers la physique. Elles reprennent des communications données en mars 1998 dans le cadre d'un colloque coorganisé par l'IREM Paris VII.

Les passionnés de Leibniz trouveront dans ce premier tome de quoi se délecter, avec trois articles de Eberhard Knobloch, Michel Serfati et Jacques Bouveresse. Les deux premiers articles « Déterminants et élimination chez Leibniz » (Knobloch) et « Mathématiques et pensée symbolique chez Leibniz » (Serfati) explorent en détail l'aspect « caractéristique combinatoire » et les tâtonnements d'une pensée à la recherche de structures et de méta-concepts, si neuve pour l'époque. Inscrite dans une doctrine métaphysique de l'harmonie, cette démarche suscite de nombreux échos jusque dans la pensée mathématique contemporaine. Le troisième article « Mathématiques et logique chez Leibniz », étudie l'influence de Leibniz sur Gödel et s'interroge sur ce qui rend si actuelles les idées de Leibniz en logique, sur la démonstration et la démontrabilité, la formalisation, la dialectique entre mécanisation du raisonnement et liberté de l'invention mathématique.

A ce propos, et pour alimenter notre réflexion pédagogique, je ne résiste pas au plaisir de vous soumettre cette citation de Whitehead en 1911, rapportée par Bouveresse (p.245) :

« C'est un truisme profondément erroné, répété par tous les cahiers d'écriture et par des gens éminents quand ils font des discours, que nous devrions cultiver l'habitude de penser à ce que nous sommes en train de faire. C'est exactement le contraire qui est vrai. La civilisation avance en étendant le nombre des opérations importantes que nous pouvons effectuer sans y penser. Les opérations de la pensée sont comme les charges de cavalerie dans une bataille – elles sont strictement limitées en nombre, elles exigent des chevaux frais et doivent être faites uniquement dans des moments décisifs. »

Je terminerai par le sommaire de la deuxième partie (Tome 54-3 – juillet-septembre 2001):

Marc Parmentier : Démonstrations et infiniment petits dans *la Quadratura arithmetica* de Leibniz

Michel Blay : De l'apparition subreptice des futures formules de conservation à l'occasion de l'algorithmisation de la science du mouvement des XVII^{e} et XVIII^{e} siècles.

Laurence Devillairs : Immutabilité divine et principe de la conservation de la quantité de mouvement chez Descartes et les éléments de la critique leibnizienne.

Carl Friedrich Gauss

Riemann

CONTE DU LUNDI II

Rudolf BKOUCHE

Riemann au carrefour de la physique, de la géométrie et de la philosophie

Contrairement à l'idée couramment répandue selon laquelle les mathématiques sont un outil pour la physique, on pourrait dire qu'avec la révolution galiléenne la physique est devenue une partie des mathématiques, et ce d'au moins trois façons :

- la physique prend une forme hypothético-déductive analogue à celle des *Eléments* d'Euclide.
- au temps-devenir des Grecs est substitué un temps géométrisé que l'on peut représenter pas une droite[1], *un temps statique* pourrait-on dire.
- sous la double impulsion des constructions perspectivistes et de l'étude du mouvement, les philosophes de la nature inventent le concept d'un espace vide, infini, triplement étendu indépendant des corps qu'il contient et des phénomènes qui s'y déroulent, espace qui satisfait les propriétés de la géométrie euclidienne[2].

Cet espace euclidien, invention des mathématiciens-physiciens du XVIIème siècle sera remis en question au début du XIXème siècle avec la découverte (l'invention !) des géométries non-euclidiennes.

Le postulat des parallèles a posé problème aux géomètres à la fois par son manque d'évidence et par sa nécessité, puisque c'est lui qui permet l'usage de la méthode des aires et de la théorie des proportions géométriques, ce qui explique les nombreuses tentatives de le démontrer[3]. Au XVIIIème siècle nous citerons les travaux de Saccheri et de Lambert.

Saccheri[4] considère un quadrilatère *ABCD* dont les côtés *AD* et *BC* sont égaux et perpendiculaires au côté *AB* (quadrilatère déjà étudié par Umar Al-Khayyam[5]) on montre aisément que les angles en *C* et *D* sont égaux. Trois cas sont alors possibles, ces angles sont droits, aigus ou obtus, le cas des angles droits correspondant à la géométrie euclidienne. On élimine l'hypothèse de l'angle obtus contradictoire au fait que l'on peut toujours prolonger une droite, reste alors à éliminer l'hypothèse de l'angle aigu ce que Saccheri ne peut faire. Il termine son ouvrage en affirmant que les conséquences de cette hypothèse sont incompatibles avec l'idée de ligne droite.

Quant à Lambert[6], il considère un quadrilatère ayant trois angles droits, posant la question du quatrième angle (cette situation avait déjà été étudiée par Ibn Al-Haytham[7]). Ici encore trois cas sont possibles, l'angle droit correspond à la géométrie euclidienne, le cas de l'angle obtus étant incompatible avec le fait que l'on peut toujours prolonger une droite. Lambert étudie alors les conséquences de l'hypothèse de l'angle aigu, en particulier les relations trigonométriques dans un triangle. Comparant ces relations avec celles que satisfait un triangle sphérique il montre que l'hypothèse de l'angle obtus correspond à la géométrie sphérique et que l'hypothèse de l'angle aigu correspond à la géométrie d'une sphère de rayon imaginaire. Lambert a ainsi mis en place les propriétés de ce qui sera la géométrie non-euclidienne mais cette sphère de rayon imaginaire ne saurait représenter le plan de notre perception (le plan physique si l'on veut).

---

[1]Isaac Newton, *The Principles of Natural Philosophy* (1686) Motte's translation revised by Cajori, University of California Press, Berkeley 1962, p. 6

[2]*ibid.* p. 6

[3]Pour une histoire de la théorie des parallèles, nous renvoyons à l'ouvrage classique de Roberto Bonola, *La Geometria non-Euclidea* (1912), english translation by H. S. Carslaw, *Non-euclidean geometry*, Dover Publications, New York 1955. Signalons l'anthologie de Jean-Claude Pont, *L'Aventure des Parallèles*, Peter Lang, Berne 1986 ; si cet ouvrage nous semble contestable sur le plan épistémologique, il offre un vaste panorama des tentatives de démonstration du postulat des parallèles depuis les Grecs jusqu'à l'époque moderne, lesquelles nous éclairent sur la signification autant géométrique qu'épistémologique du postulat et du "besoin" de le démontrer. Enfin pour les travaux des mathématiciens arabes sur ce sujet nous renvoyons, outre les ouvrages cités, à l'ouvrage de K. Jaouiche, *La théorie des Parallèles en Pays d'Islam*, Vrin, Paris 1986.

[4]H. Saccheri, *Euclides ab omni nævo vindicatus*, Milano 1733

[5]Umar Al-Khayyam in K. Jaouiche, o.c. p. 185-199

[6]J.H. Lambert, *Theorie der Parallellienen*, Leipzig 1786

[7]Ibn Al-Haytham in Jaouiche, o.c. p. 161-184

La géométrie non-euclidienne naîtra lorsque des géomètres considèreront que l'hypothèse non-euclidienne peut s'appliquer au plan physique, autrement dit si la physique peut être non-euclidienne ; ce sera l'objet des travaux de Gauss, Bolyai et Lobatchevski[8]. L'apparition des géométries non-euclidiennes conduira à l'idée d'une multiplicité de géométries, ce qui posera un double problème : problème physique d'une part : quelle est la géométrie de l'espace ? problème logique d'autre part : s'il y a une multiplicité de géométries, comment assurer la rigueur du raisonnement si l'on sait la part d'intution qui sous-tend le raisonnement géométrique. Le problème logique sera réglé lorsque l'on construira des modèles euclidiens de géométries non-euclidiennes (Klein, Poincaré) lesquels montreront que toute contradiction de la géométrie non-euclidienne implique une contradiction dans la géométrie euclidienne. Quant au problème physique il donnera lieu à de nombreux travaux dont le texte de Riemann est un point essentiel. Notons que la possibilité d'une géométrie non-euclidienne donnera longtemps lieu à controverse comme le montrent les réticences de Cayley[9] et de Frege[10].

La mise en évidence d'une multiplicité de géométries va conduire à penser une multiplicité d'espaces possibles, ce qui permettra de reformuler le problème physique sous la forme suivante : parmi les espaces possibles, lequel est l'espace physique ? Cette question exige de définir ce que peut être un concept général d'espace et c'est ce que propose Riemann dans le texte d'habilitaion de 1854 : *Sur les Hypothèses qui servent de Fondement à la Géométrie*[11]. Ce texte, l'un des plus beaux et des plus difficiles de l'histoire des mathématiques, se situe au carrefour de la géométrie, de la physique et de la philosophie.

Ce texte est le discours d'habilitation prononcé par Riemann devant les professeurs de l'Université de Göttingen, ce qui explique en partie le caractère non technique de ce texte, caractère non technique qui n'en rend pas la lecture plus aisée.

Si le concept d'espace est à redéfinir, Riemann se propose, dans une démarche que l'on peut considérer proche de celle de Leibniz, de chercher à définir le concept général d'espace avant d'étudier l'espace physique en tant que tel. Cela l'amène à distinguer parmi les propriétés de l'espace les propriétés métriques de celles qui concernent la notion générale de grandeur étendue ; c'est seulement après avoir défini ces deux types de propriétés que Riemann aborde la question de l'espace physique, renvoyant à l'expérience pour décider parmi les diverses propriétés possibles celles qui correpondent à l'espace physique. Aboutissement des recherches liées à la découverte des géométries non euclidiennes, Riemann passe ainsi de la notion d'espace à la notion d'espaces.

Si, à l'époque où il écrivait sa dissertation, Riemann s'intéressait à des problèmes de physique, ceux-ci n'apparaissent pas en tant que tels dans son texte, même si la physique est présente dans tout le texte, et pas seulement dans la dernière partie consacrée à ce que l'on appelle l'espace physique ; ce que Riemann nous propose, c'est une promenade à travers ces nouveaux espaces qu'il présente, promenade au sens que cette présentation propose un élargissement de l'intuition spatiale usuelle comme le montre sa description des espaces multidimensionnels. Mais cet élargissement de l'intuition est lui-même préparé par un texte antérieur de Gauss publié en 1827 : *Disquisitiones Generales circa Superficies Curvas*[12] ; la notion de surface y apparaît autant dans son aspect intuitif que dans la représentation qu'en propose Gauss mettant en place les coordonnées curvilignes et les calculs correspondants. C'est *via* ces calculs que Gauss va faire la découverte qui conduit à l'*egregium theorema*, lequel va permettre de penser la notion de surface abstraite.

Gauss se propose de calculer la courbure d'une surface et pour cela s'appuie sur une construction relative aux courbes planes. On considère un arc de courbe AB et, un point O étant donné dans le plan, on associe à tout point M de l'arc AB le point T_M tel que le segment OT_M soit parallèle à la tangente au point M, orienté dans le sens AB et unitaire (en langage moderne on dira que le $\boldsymbol{OT}_M$ est égal au vecteur unitaire tangent en M à l'arc de courbe AB orienté de A vers B), lorsque M parcourt l'arc AB, le point T_M parcourt un arc de cercle ; si l'on note s la longueur de l'arc AM et σ la longueur de l'arc de cercle T_AT_M, la courbure au point A n'est autre que la limite de σ/s lorsque le point M tend vers le point A. Notons qu'au lieu de prendre la tangente on aurait tout aussi bien pu prendre la normale, une fois les questions d'orientation précisées. Gauss propose une construction analogue pour les surfaces.

Notons d'abord qu'une surface Σ étant donnée rapportée à des coordonnées curvilignes (p,q), on détermine l'élément linéaire dont le carré est défini par la forme quadratique

---

[8]Pour ces travaux nous renvoyons à l'ouvrage cité de Bonola.

[9]A. Cayley, "Presidential Adress to the British Association, September 1883" Report of the British association of Science" 1883, p. 3-37 ; n°784 in *Collected Mathematical Papers*, o.c. vol. XI, p. 429-459

[10]G. Frege, "Sur la géométrie euclidienne" in *Ecrits posthumes*, traduits de l'allemand sous la direction de Philippe de Rouilhan et Claudine Tiercelin, Editions Jacqueline Chambon, Nîmes 1994, p. 199-201

[11]Bernhart Riemann, "Sur les hypothèses qui servent de fondement à la géométrie", traduction Jules Houël, in *Oeuvres Mathématiques*, Blanchard, Paris 1968, réédition Gabay, Paris 1990

[12]Signalons une traduction française par Roger, *Remarques générales sur les surfaces courbes*, ré-édition Blanchard, Paris 1967, et une traduction anglaise par P. Dombrowski in *150 Years after Gauss*, Astérisque 62, Société Mathématique de France, Paris 1979.

$$ds^2 = Edp^2 + Fdpdq + Gdq^2$$

qui donne la distance entre les deux points de coordonnées (p,q) et $(p+dp,q+dq)$. On peut alors calculer la longueur d'une ligne tracée sur la surface et l'angle de deux lignes au point où elles se coupent. On peut aussi, utilisant le calcul des variations, déterminer la ligne de plus courte distance (géodésique) qui joint deux points.

Pour étudier la forme de la surface Gauss introduit l'application suivante (aujourd'hui connue comme l'application de Gauss). Soit O un point donné de l'espace, on associe à tout point M de cette surface le point N_M tel que le segment ON_M soit parallèle à la normale au point M, le sens de la normale étant défini par un côté de la surface fixé une fois pour toutes, et unitaire. Lorsque le point M parcourt un morceau de la surface Σ le point N_M parcourt un morceau de la sphère unitaire de centre O. On associe ainsi à tout morceau de la surface un morceau de sphère et Gauss appelle *courbure intégrale* d'un morceau de surface le quotient de l'aire du morceau de sphère correspondant sur l'aire du morceau de surface donné. Un point A de la surface étant donné, si l'on note S l'aire d'un morceau de surface entourant le point A et σ l'aire du morceau de sphère correspondant, Gauss appelle *mesure de la courbure* au point A la limite du rapport σ/S lorsque le morceau entourant A devient infiniment petit, on retrouve ainsi la courbure précédemment définie par Euler. Par analogie avec les courbes on peut considérer que la mesure de la courbure représente la forme de la surface dans l'espace, or Gauss a montré que la mesure de la courbure ne dépend que de la première forme fondamentale de la surface, celle qui permet de calculer les longueurs et les angles des courbes tracées sur la surface ; ainsi si l'on déforme isométriquement une surface la mesure de la courbure ne change pas même si la forme change[13], par exemple un plan et un cône ont même mesure de la courbure, soit 0. La mesure de la courbure définit donc une grandeur intrinsèque indépendante de la forme de la surface dans l'espace, ce que l'on appellera une *grandeur géodésique*. Le théorème de Gauss, que celui-ci appelle *egregium*, c'est-à-dire remarquable[14], conduit à penser une géométrie intrinsèque des surfaces définies par la première forme fondamentale et les grandeurs géodésiques. On ne peut douter que, bien qu'il n'ait jamais rien publié sur les géométries non-euclidiennes[15], Gauss a compris le lien entre sa théorie des surfaces et les questions de géométrie non euclidienne comme le montre le calcul de la somme des angles d'un triangle géodésique où la courbure intervient, ce qui permettra ultérieurement de redéfinir la géométrie non-euclidienne comme celle s'une surface à courbure constante[16]. Cette redéfinition de la géométrie des surfaces et le développement de la géométrie non-euclidienne conduiront Gauss à poser le problème de l'espace sous une forme nouvelle et on comprend pourquoi Gauss ait tenu à ce que Riemann aborde ce sujet[17].

Comme nous l'avons déjà dit Riemann, pour aborder le problème de l'espace, va poser la question de la construction du concept d'espace, c'est seulement le concept une fois défini que l'on peut en expliciter les développements théoriques et voir ensuite comment ce concept peut intervenir en physique. On peut comparer la démarche de Riemann à celle de Leibniz se proposant de définir les grandeurs géométriques à partir du seul raisonnement et de construire *a priori* les êtres de raison qui lui permettront d'étudier le monde[18].

Riemann divise son exposé en trois parties, la première est consacrée à la notion générale de grandeur multidimensionnelle (*mannigfaltigkeit*)[19], la seconde s'intéresse aux propriétés métriques et c'est dans la troisième partie que Riemann pose le problème de l'espace.

Dans la première partie Riemann définit le concept de grandeur n-fois étendue. Il remarque alors que ce concept est indépendant de tout rapport métrique, renvoyant sans autre explication à des travaux antérieurs[20]. Il

---

[13]plus généralement si deux surfaces sont applicables l'une sur l'autre les mesures de courbure en deux points correspondants sont égales.

[14]littéralement : qui sort du troupeau

[15]par peur des cris des Béotiens comme il l'écrit à Bessel en1829.

[16]On peut citer ici les travaux de Minding (*Journal de Crelle*, vol XIX. 1839, p. 370-387 et vol. XX, 1840, p. 323-327) et de Beltrami ("Saggio di interpretazione della geometria non-euclidea", *Giornale di Matematica* 6, 1868, p. 284-312, traduction française, "Essai d'interprétation géométrique de la géométrie non-euclidienne", *Annales de l'ENS*, tome V, 1868, p. 251-288). Pour une étude systématique des relations entre géométrie différentielle nous renvoyons à l'ouvrage de L. Boi, *Le problème mathématique de l'espace*, avec une préface de René Thom, Springer, Berlin-Heidelberg-New York 1995.

[17]Alors que Riemann avait le choix entre trois sujets Gauss lui a imposé ce sujet.

[18]Pour Leibniz l'espace, *ordre des coexistences*, est un être de raison, une construction intellectuelle. C'est cette construction intellectuelle qui permet d'étudier les problèmes du monde, (*Correspondance Leibniz-Clarke*, présentée par André Robinet, PUF, Paris 1957, p. 53). En un sens, la notion d'espace comme *ordre des coexistences* est proche de l'invention de l'espace par les perspectivistes de la Renaissance comme mode de coordination des divers lieux qui interviennent dans les problèmes de représentation.

[19]les variétés différentiables de la géométrie différentielle

[20]Parmi ces travaux il cite, sans plus de détails, ceux de Lagrange, Abel, Pfaff et Jacobi.

explique alors que dans cette branche générale de la théorie des grandeurs *"on ne suppose rien de plus que ce qui est déjà renfermé dans le concept de ces grandeurs"*. Pour préciser cette affirmation il explicite les deux points qu'il va développer dans cette première partie, le premier portant sur *"la génération du concept de variété à n dimensions"*, le second sur *"le moyen de ramener les déterminations de lieu dans une variété donnée à des déterminations de quantités"* et il ajoute : *"c'est ce dernier point qui doit faire clairement ressortir le caractère essentiel d'une étude à n dimensions"*.

Pour définir la dimension Riemann rappelle que le mouvement d'un point engendre une ligne, que le mouvement d'une ligne engendre une variété à deux dimensions et que le mouvement d'une telle variété engendre une variété à trois dimensions. Il ajoute alors, et c'est l'un des points essentiels de sa conférence : *"... il est aisé de voir comment on peut poursuivre cette construction"*, ce qui lui permet d'écrire :

"Si, au lieu de considérer le concept comme déterminable, on considère son objet comme variable, on pourra désigner cette construction comme la composition d'une variabilité de n+1 dimensions, au moyen d'une variabilité de n dimensions et d'une variabilité d'une seule dimension."

On peut noter ici le pas effectué par Riemann dans une construction qui relève plus d'un élargissement de l'intuition que d'une définition analytique. Elargissement de l'intuition spatiale qui permet de concevoir le mouvement comme une opération générale qui permet d'augmenter la dimension *ad libitum*. Dans ses écrits sur la caractéristique géométrique, Leibniz faisant une remarque analogue sur le mouvement d'un point, d'une ligne ou d'une surface n'osait pas imaginer qu'un volume puisse sortir de l'espace pour engendrer un objet d'une dimension plus grande ; c'est ainsi qu'après avoir défini une trajectoire comme *"un lieu continu successif"* et remarqué que la trajectoire d'un point est une ligne, il écrit :

"La trajectoire d'une ligne, dont les points ne prennent pas constamment la place les uns des autres, est une ***Surface****. Celle d'une surface dont les points ne prennent pas toujours la place les uns des autres, est un* ***Corps****. Un corps quant à lui ne peut être mû sans que tous ses points prennent la place les uns des autres (il faudra démontrer pourquoi le moment voulu) et ce mouvement ne produit aucune nouvelle dimension"*[21]

Dans un texte ultérieur, Leibniz explique que si un point peut être l'extrémité d'une ligne, un ligne peut être l'extrémité d'une surface et une surface l'extrémité d'un solide, *"un solide ne peut plus être l'extrémité de quelque chose d'autre"*[22]

Ainsi le rationaliste Leibniz reste enfermé dans la connaissance sensible[23] alors que Riemann, plus proche de l'empirisme, propose moins une définition rationnelle de ces nouveaux espaces qu'un élargissement de l'intuition sensible, ouvrant ainsi un nouveau champ d'étude. Cela remet en question la classique, et facile, opposition entre empirisme et rationalisme si l'on considère que l'activité scientifique se situe au carrefour de l'empirisme et du rationalisme, permettant à la fois un élargissement de l'intuition sensible et la construction d'un discours rationnel qui assure à son tour une meilleure prise sur le sensible.

Une fois définie la notion de grandeur multidimensionnelle, Riemann explique comment définir des systèmes de coordonnées : une fonction continue[24] sur une multiplicité de dimension n permet d'y distinguer des multiplicités de dimensions n-1, une telle multiplicité étant le lieu des points où cette fonction prend une valeur constante ; un mouvement inverse du mouvement d'engendrement permet ainsi d'établir la possibilité de repérer les éléments d'une multiplicité abstraite à n dimensions par n fonctions numériques jouant le rôle de coordonnées. Notons que Riemann ne s'embarrasse pas des difficultés liées à ce que nous appellerions aujourd'hui la transversalité, se contentant d'annoncer : *"Les cas d'exception, dont l'étude est importante, peuvent être ici laissés de côté"*.

Ici encore tout se joue sur le qualitatif, y compris la construction du quantitatif. La façon dont s'élabore un concept est ici plus importante que les constructions analytiques ou formelles qui en seront données plus tard, constructions certes nécessaires mais c'est la définition qualitative qui donne sa force au concept[25].

---

[21]G.W. Leibniz, *la caractéristique universelle*, texte établi, introduit et annoté par Javier Echeverria, traduit, annoté et postfacé par Marc Parmentier, "Mathesis", Vrin, Paris 1995, p. 155

[22]*ibid.* p. 285

[23]On peut considérer le travail de Leibniz sur la caractéristique géométrique comme une tentative de construire une méthode rationnelle permettant de se dégager du sensible pour mieux l'étudier, mais ce travail demande de rester proche du sensible.

[24]il faut prendre ici la notion de continuité dans son sens intuitif.

[25]Dans un article ultérieur Riemann s'appuiera sur des constructions analytiques mais nous n'en parlerons pas ici. cf. Bernhardt Riemann, "Commentatio mathematica, qua respondere tentatur quæstioni ab III[ma] Academia Parisiensi propositiæ" (1864) in *Riemann's Gesamm. Math. Werke* XXII, 2, Aufl. (1892), p. 391-423

La notion de grandeur multidimensionnelle une fois mise en place, Riemann peut aborder dans une deuxième partie la question des rapports métriques.

Après être revenu sur *"l'indépendance entre les grandeurs et le lieu"*, Riemann va déterminer les rapports métriques dans l'infiniment petit ce qui le conduit à définir l'*élément linéaire* (distance de deux points infiniment voisins) *ds* comme une grandeur homogène du premier degré des accroissement[26] *dx* des coordonnées *x* ; l'élément linéaire étant une grandeur positive, *ds* peut être défini comme la racine nième d'une forme homogène de degré pair n en les accroissements *dx*. Rieman s'intéresse ici au seul cas où l'élement linéaire *ds* est la racine carrée d'une forme quadratique[27], soit $ds=\sqrt{\sum g_{ij}dx_i dx_j}$. On peut imaginer des cas plus généraux qui *"n'exigeraient pas des principes essentiellement différents"* mais compliqueraient les calculs.

Le cas classique est évidemment celui des variétés planes pour lequel l'élément linéaire peut s'écrire dans un système de coordonnées convenables

$$ds=\sqrt{\sum dx_i^2}$$

mais on sait que tout élément linéaire ne peut en général se ramener à cette forme.

On voit ici se poser d'abord le problème de la caractérisation des variétés planes, ensuite le problème de l'équivalence de deux éléments linéaires.

Un élément linéaire étant donné, on peut alors déterminer les éléments métriques : longueur d'un arc de courbe, angle de deux courbes se rencontrant en un point. En particulier on peut définir les géodésiques (courbes de plus courte distance entre deux points) et le calcul des variations montre qu'entre deux points suffisamment voisins, il existe une géodésique et une seule les joignant.

Pour caractériser les variétés qu'il vient de définir, Riemann, s'appuyant sur l'article cité de Gauss, se propose de définir la *mesure de courbure*. Pour cela il introduit, à la façon de Gauss, les coordonnées géodésiques : un point étant donné (point-origine), on considère les lignes géodésiques (lignes de plus courte distance) issues de ce point, *"la position d'un point indéterminé pourra être fixée alors au moyen de la direction initiale de la ligne de plus courte distance sur laquelle il se trouve et de sa distance comptée sur cette ligne à partir de l'origine et par conséquent elle pourra s'exprimer au moyen des rapports dx^0 des quantités dx sur cette ligne de plus courte distance et au moyen de la longueur s de cette ligne"*. On peut alors construire un système de coordonnées tel que les lignes coordonnées passant par le point-origine soient orthogonales et que le développement du carré de l'élément linéaire au voisinage du point *O* soit tel que le terme du second ordre s'écrive Σdx_i^2 et le terme du quatrième ordre s'écrive $\Sigma\rho_{ij}(x_i dx_j - x_j dx_i)^2$, les termes ρ_{ij} représentant la *mesure de la courbure* de la surface définie par le triangle géodésique infiniment petit dont les sommets sont le point origine, le point de coordonnées $(x_1,x_2,\ldots,x_n)$ et le point infiniment voisin $(dx_1,dx_2,\ldots,dx_n)$[28]. Ce terme est évidemment nul lorsque la variété est plane.

A côté des variétés planes, Riemann s'intéresse aux variétés dont la mesure de la courbure est constante, il remarque que sur de telles variétés *"les figures peuvent s'y mouvoir sans subir d'extensions"*, propriété qu'il ne démontre pas se contentant de montrer qu'elle n'est pas satisfaite pour une variété dont la mesure de la courbure n'est pas constante. Il montre de plus que sur une variété à courbure constante la métrique est déterminée par la mesure de la courbure. Il termine cette seconde partie en étudiant le cas des surfaces[29].

Enfin dans la troisième partie, Riemann aborde la question de l'espace.

Riemann explique que les propriétés de l'espace se définissent essentiellement dans l'infiniment petit et pose alors une série d'alternatives .

Soit l'espace est discret, auquel cas l'étude de l'espace est une question de dénombrement, soit l'espace est continu et dans ce cas son étude relève de la théorie générale qu'il a exposée.

Dans ce dernier cas il remarque que si *"les corps existent indépendamment du lieu, la mesure de courbure est constante"*, autrement dit la géométrie ne dépend pas de la distribution des corps dans l'espace. Il

---

[26]en termes modernes on pourrait parler de différentielles !

[27]ce qui correspond au théorème de Pythagore.

[28]Riemann signale que pour retrouver la courbure de Gauss il faut mulitplier les coefficients ρ_{ij} par –3/4.

[29]Une étude générale des variétés à courbure constante sera publiée par Beltrami ("Teoria fondamentale degli spazii di curvatura constante", *Annali di Matematica pura ed applicata*, 2ème série, tome II, 1868-1869, p. 232-255, traduction française, "Théorie fondamentale des espaces à courbure constante", *Annales de l'ENS*, tome VI, 1868-69, p. 347-375). Ce travail fait suite à son essai d'interprétation de la géométrie non-euclidienne (cité note 10), lequel s'appuie sur les travaux de Gauss sur les surfaces et se propose d'interpréter en termes de géométriie différentielle les travaux de Lobatchevski. Beltrami avait écrit ce texte avant de connaître le texte de Riemann, après avoir lu celui-ci il généralisait son essai aux variétés de dimension quelconque.

explique alors, sans autre précision, que les mesures astronomiques impliquent que la mesure de courbure est nulle, autrement dit que l'espace est une variété plane.

Si par contre *"l'indépendance entre les corps et le lieu n'existe pas"*, c'est-à-dire si la présence de corps influe sur la géométrie de l'espace, alors la mesure de courbure est variable.

Il résume ainsi l'alternative :

"Il faut donc, où que la réalité sur laquelle est fondée l'espace forme une variété discrète, ou que le fondement des rapports métriques soit cherché en dehors de lui, dans les forces de liaison qui agissent en lui"

Arrivé à ce point, Riemann renvoie à l'expérience. Si la recherche de concepts généraux est nécessaire pour que le travail sur la géométrie de l'espace ne soit pas entravé par des vues trop étroites et les préjugés traditionnels comme il l'explique à la fin de sa conférence, la détermination de cette géométrie relève d'un autre domaine, celui de la Physique. On voit que subsiste ici l'idée que parmi toutes les géométries possibles que propose le travail de Riemann il en existe une qui correspond à la réalité. Il faudra attendre la critique de Poincaré pour qu'apparaisse l'idée que le problème est moins de trouver la vraie géométrie que de chercher comment une géométrie peut nous parler du monde[30].

Le texte de Riemann aura une double postérité, mathématique d'une part avec la théorie des variétés différentiables, physique d'autre part, laquelle se manifestera par les relations étroites entre la géométrie différentielle et la physique mathématique. Cette postérité physique peut elle-même se diviser en deux parties, la première concernant la structure géométrique de l'espace puis de l'espace-temps après la naissance des théories relativistes, la seconde conduisant à la *géométrisation* de certains chapitres de la mécanique et de la physique. Ces diverses postérités s'entremêleront pour fonder une théorie générale des espaces.

Sur un plan strictement mathématique nous pourrons citer les problèmes que l'on appelle aujourd'hui *problèmes d'équivalence*. Dans le cas des variétés riemanniennes un tel problème se présente ainsi :

Soient deux variétés rapportées respectivement aux coordonnées $(x_1,x_2,\ldots,x_n)$ et $(y_1,y_2,\ldots,y_n)$ et les éléments linéaires correspondants

$$ds^2 = \Sigma g_{ij}dx_i dx_j \qquad dt^2 = \Sigma h_{lm}dy_l dy_m$$

Nous dirons qu'elles sont équivalentes s'il existe une transformation de coordonnées

$$y_l = f_l(x_1,x_2,\ldots,x_n)$$

qui envoie la seconde forme différentielle quadratique sur la première.

La détermination des conditions d'équivalence de deux structures riemanniennes conduira à la définition d'un invariant tensoriel, aujourd'hui appelé le tenseur de courbure ou le tenseur de Riemann-Christoffel introduit par Riemann dans l'article cité de 1864. On montre alors que deux structures riemanniennes équivalentes définissent le même tenseur de courbure. En particulier un espace est localement euclidien si et seulement si son tenseur de courbure est nul. Le problème d'équivalence sera étudié systématiquement par Christoffel[31] qui introduira les symboles qui portent son nom. Ces symboles joueront un rôle essentiel dans la construction de la notion de dérivation covariante par Ricci[32].

En ce qui concerne le problème physique de l'espace, nous nous contenterons de citer Clifford qui pose la question de ce que peut signifier la courbure de l'espace. Ceci l'amène à écrire les remarques suivantes :

"That small portions of space ***are*** *in fact of a nature analogous to little hills on a surface which is on the average flat; namely, that the ordinary laws of geometry are not valid in them.*

That this property of being curved or distorted is continually being passed on from one portion of space to another after the manner of a wave.

That this variation of the curvature of space is what really happens in that phenomenon which we call the ***motion of matter****, whether ponderable or etherial.*

That in the physical world nothing else takes place but this variatio

---

[30]H. Poincaré, *La Science et l'Hypothèse* (1902), préface de Jules Vuillemin, Flammarion, Paris 1968, deuxième partie : l'espace.

[31]Christoffel, *Journal de Crelle*, 70, 1869, p. 6-70 et 241-245

[32]G. Ricci, "Delle derivazione covarianti e contravarianti" *Studi éditi dell' Univcersità di Padova ecc*, Padova 1888 et "Résumé de quelques travaux sur les systèmes variables de fonctions associés à une forme différentielle quadratique", *Bulletin des Sciences Mathématiques*, 2ème série, tome XVI, 1892 p. 167-189

n subject (possibly) to the law of continuity."[33]

Cette notion de courbure de l'espace définie par l'influence des corps sur la géométrie de l'espace fera son chemin pour aboutir à la théorie de la Relativité Générale d'Einstein en 1916.

Mais de façon plus générale d'étroites relations se construisent entre la géométrie différentielle issue des travaux de Riemann et la physique mathématique comme le montre l'article de Ricci et Levi-Civita sur le calcul différentiel absolu[34]. A côté du problème de la structure de l'espace se met en place ce que nous avons appelé ci-dessus une géométrisation de la mécanique dont l'un des premiers exemples est donné par la reformulation géométrique de la mécanique analytique lagrangienne par Levi-Civita[35].

L'étude des équations de Lagrange avait conduit à étudier les conditions pour que deux systèmes mécaniques soient équivalents au sens où l'intégration des équations de Lagrange du premier système permet l'intégration des équations de Lagrange du second système, problème posé dans un cadre purement analytique[36]. Levi-Civita montrera l'aspect géométrique de ce problème et sa relation avec l'équivalence des variétés riemanniennes.

Un système mécanique à n degrés de liberté peut être représenté par un point d'une variété de dimension n. On note $(x_1,x_2,\ldots,x_n)$ un système de coordonnées, alors la cinétique du système est définie par son énergie cinétique T qui est une expression quadratique en les vitesses $(v_1,v_2,\ldots,v_n)$ du système où pour tout indice i

$$v_i=\frac{dx_i}{dt}$$

L'énergie cinétique T est alors définie par la relation

$$2T = \Sigma a_{ij}v_iv_j$$

Le problème de la transformation des équations de la dynamique peut alors être posé sous la forme suivante : étant donnés deux systèmes dynamiques respectivement définis par les systèmes $(x_1,x_2,\ldots,x_n)$ et $(y_1,y_2,\ldots,y_n)$ et les énergies cinétiques

$$2T = \Sigma a_{ij}v_iv_j \qquad\qquad 2U = \Sigma b_{lm}w_lw_m$$

peut-on trouver un changement de variables

$$y_l = f_l(x_1,x_2,\ldots,x_n)$$

qui transforme U en T ?

Levi-Civita remarque l'analogie avec le problème de l'équivalence de deux structures riemanniennes. Pour préciser cette analogie il introduit l'espace de configuration du système comme la variété définie par les paramètres de définition du système qu'il munit de la métrique définie par la forme quadratique

$$ds^2 = \Sigma a_{ij}v_iv_j$$

Il remarque ensuite que le terme cinétique des équations de Lagrange n'est autre que la dérivée covariante de la vitesse dans l'espace de configuration ce qui conduit à une reformulation géométrique de ces équations. En particulier pour un système libre (non soumis à des forces extérieures) la dérivée covariante de la vitesse est nulle ce qui implique que le point représentant le système dans l'espace de configuration décrit une géodésique d'un mouvement uniforme. On peut considérer ce résultat comme une généralisation du principe d'inertie.

Ainsi la mécanique analytique de Lagrange redevenait une théorie géométrique, à condition de considérer l'espace de configuration du système ; on peut ainsi parler de *géométrisation* de la mécanique, ce qui

---

[33]W. K. Clifford, "On the Space Theory of Matter" (1876), in James R. Newman, *The World of Mathematics*, Tempus 1988, volume one, p. 559-560

[34]G. Ricci, T. Lévi-Civita, "Methodes de calcul différentiel absolus et leurs applications", *Mathematische Annalen*, Band 54, 1901, p. 125-201

[35]T. Levi-Civita, "Sulla tranformazione delle equazioni dinamiche", *Annali di matemetica pura ed applicata*, Serie II, Tomo XXIV, 1896, p. 255- 300

[36]C'est le problème de la transformation des équations de la dynamique étudié tout au long du XIXème siècle.

permet de considérer celle-ci comme un chapitre de la géométrie différentielle, point de vue qui est à la source de nombreux travaux toujours actuels[37].

Ainsi se met en place une profonde symbiose entre la géométrie différentielle et la physique qui a marqué l'évolution conjointe de ces deux domaines tout au long du XXème siècle[38]. Nous pouvons ici citer parmi les ouvrages classiques mettant en valeur cette symbiose, d'abord le classique *Raum, Zeit, Materie* (traduction anglaise *Space, Time, Matter*[39]) de Hermann Weyl, ensuite dans la seconde partie du XXème siècle l'ouvrage de André Lichnérowicz, *Théories Relativistes de la Gravitation et de l'Electromagnétisme*[40] ainsi que celui de Vladimir Arnold déjà cité.

Nous terminerons cet exposé en citant Reichenbach qui écrivait en 1927 :

"Mathematics reveals the possible espaces; physics decides which among them corresponds to physical space"[41]

Notons la double interprétation du terme *"decides"* ; soit l'espace physique a une structure géométrique déterminée et le physicien doit découvrir cette structure parmi les possibles, soit la structure est déterminée par le physicien pour rendre compte des phénomènes ; la préface de Carnap laisse entendre que c'est la seconde interprétation qu'il faut lire:

"In physical geometry, there are two possible procedures for establishing a theory of physical space. First, the physicist may freely choose the rules for measuring length. After this choice is made, the question of the geometrical structure of physical space becomes empirical ; it is to be answered on the basis of the results of experiments. Alternatively, the physicist may freely choose the structure of physical space ; but he must adjust the rules of measurement in view of the observational facts."[42]

Ainsi la géométrie différentielle issue des conceptions de Riemann sur l'espace devient l'un des lieux où s'élabore la physique, ce qui nous permet encore une fois d'insister sur le caractère mixte des mathématiques, à la fois dans le monde et hors du monde. Mais c'est bien parce qu'elles savent se placer hors du monde que les mathématiques peuvent nous parler du monde et le texte de Riemann est une parfaite illustration de ce que Wigner a appelé *"la déraisonnable efficacité des mathématiques"*[43].

---

[37]V. Arnold, *Méthodes mathématiques de la Mécanique Classique* (1974), traduit du russe par Djilali Embarek, Editions Mir, Moscou 1976

[38]Pour une histoire des liens entre géométrie et physique nous renvoyons à l'article de Christian Houzel, "Géométrie et Physique" in *Universalia* 1991, supplément annuel à *Encyclopædia Universalis*

[39]Hermann Weyl, *Space, Time, Matter* (1918), translated from the German by Henry L. Brose, Dover Publications, Inc., New York 1952

[40]André Lichnérowicz, *Théories relativistes de la Gravitation et de l'Electromagnétisme*, "Collection d'Ouvrages de Mathématiques à l'Usage des Physiciens", Masson, Paris 1955

[41]Hans Reichenbach, *The Philosophy of Space and Time* (1927) (translated by Maria Reichenbach and John Freund, with introductory remarks by Rudolf Carnap), Dover, New York 1957, p. 6

[42]*ibid.* p. vi

[43]E.P. Wigner, "The unreasonable effectiveness of mathematics in the natural sciences", *Comm. Pure and Applied Math.* 13, 1960, p. 1-14

Le groupe M.:A.T.H.

(Mathématiques: Approche par les Textes Historiques)

vous propose:

La revue Mnémosyne pour échanger expériences et réflexions à propos de l'histoire et de l'enseignement des mathématiques.

Numéro 1 :	La démonstration par exhaustion chez les grecs et les arabes.	4,00 €	200 gr
Numéro 2 :	La querelle entre Descartes et Fermat.	4,50 €	210 gr
Numéro 3 :	Fragments d'étude des systèmes linéaires.	4,50 €	220 gr
Numéro 4-5 :	L'élaboration du calcul des variations et ses applications à la dynamique.	6,00 €	300 gr
Numéro 6 :	Leibniz et l'Ecole continentale.	4,50 €	220 gr
Numéro 7 :	Autour du théorème de Fermat : C. Goldstein	5,00 €	230 gr
Numéro 8 :	Isaac Newton. Détermination de tangentes à des courbes à l'aide de la méthode des fluxions.	5,00 €	250 gr
Numéro 9 :	Desargues et Pappus. R. Tossut	5,00 €	240 gr
Numéro 10 :	Le jeu des paradoxes dans l'élaboration des séries. A. Michel-Pajus	5,00 €	260 gr
Numéro 11 :	Des cartes-portulants à la formule d'Edward Wright. M.T. Gambin	5,00 €	255 gr
Numéro 12 :	Histoire de quelques projections cartographiques. M. Benedittini	5,00 €	255 gr
Numéro 13 :	Leibniz. Histoire et origine du calcul différentiel. A.Michel–Pajus	5,00 €	210 gr
Numéro 14 :	La méthode des pesées chez Archimède. M. Bathier –Fauvet	5,00 €	214 gr
Numéro 15 :	Recherche de deux grandeurs connaissant leur somme et leur produit.	5,00 €	217 gr
Numéro 16 :	De la résolution des équations algébriques à l'émergence du concept de groupe. M. Buhler	5,00 €	210 gr
Numéro spécial :	N° 1 : Histoire de Pyramides. M. Grégoire	7,00 €	380 gr

Brochures du groupe M.:A.T.H.

n° 61 : Mathématiques : Approche par des textes historiques - Tome 1 -.....	7,50 €	450 gr
n° 79 : Mathématiques : Approche par des textes historiques - Tome 2 -	9,00 €	530 gr
n° 91 : Mathématiques : Approche par des textes historiques - Tome 3 -	3,50 €	193 gr

Reproduction de textes anciens

(Ancienne série) :

I	Disme	Simon Stevin.	2,00 €	80 gr
II	Géométrie élémentaire	Félix Klein	4,00 €	180 gr
III	Dictionnaire Mathématiques	M. Ozanam (1er fascicule)	4,50 €	250 gr
IV	Dictionnaire Mathématique	M. Ozanam (2ème fascicule)	5,00 €	250 gr

(Nouvelle série) :

N° 1 : Histoire des recherches sur la quadrature du cercle	J.E Montucla	6,00 €	340 gr
N° 2 : Elémens du calcul des probabilités	Marquis de Condorcet	4,50 €	240 gr
N° 3 : Traité des Indivisibles	Gilles-Personne de Roberval	5,00 €	270 gr
N° 4 : Les Porismes d'Euclide	Michel Chasles	5,50 €	300 gr
N° 5 : Sur la théorie des Ensembles	Georg Cantor	8,00 €	450 gr
N° 6 : Traité des sections coniques	M. de La Chapelle	6,50 €	450 gr
N° 7 : Traité élémentaire de calcul des probabilités	S-F Lacroix	5,50 €	300 gr
N° 8 : Elémens d'algèbre	Alexis-Claude Clairaut	6,00 €	350 gr
N° 9 : Recueil d'exercices sur le calcul infinitésimal	Jean-Frédéric Frénet	6,50 €	384 gr
N° 10 Problèmes pour les arpenteurs	Lorenzo Mascheroni	3,00 €	156 gr
N° 11 Méthode des moindres carrés	Carl-Friedrich Gauss.....	5,50 €	295 gr
N° 12 Traité du calcul différentiel et du calcul intégral	Sylvestre-François Lacroix	10,50 €	600 gr
N° 13 Géométrie ou de la mesure de l'étendue	P. Lamy	8,00 €	395 gr
N°14 Algèbre	J.Peletier du Mans	5,50 €	291 gr

Nous vous indiquons le prix des brochures sans le port, le poids et le tarif postal pour calculer le coût du port.

Poids jusqu'à	Ordinaires
20 gr	0,46 €
50 gr	0,69 €
100 gr	1,02 €
250 gr	1,75 €
500 gr	2,44 €
1000 gr	3,20 €
2000 gr	4,27 €
3000 gr	5,03 €

✂----------

BON DE COMMANDE

Je désire recevoir les numéros suivants :

Quantité	N° et titre des documents	Prix	Port

Total:

Nom:
Prénom:
Adresse:

Date:
Ci-joint un chèque d'un montant de
A l'ordre de l'Agent comptable de l'Université Denis Diderot Paris 7
Désirez-vous recevoir une facture? Oui Non

RARA ARITHMETICA

¶ A CATALOGVE OF THE ARITHMETICS WRITTEN BEFORE THE YEAR MDCI WITH A DESCRIPTION OF THOSE IN THE LIBRARY OF GEORGE ARTHVR PLIMPTON OF NEW YORK

BY DAVID EVGENE SMITH OF TEACHERS COLLEGE COLVMBIA VNIVERSITY

GINN AND COMPANY PVBLISHERS
BOSTON AND LONDON MDCCCCVIII

Courrier à adresser à : Groupe M.: A.T.H.

IREM de l'Université Denis DIDEROT Paris VII
Case 7018
2, place Jussieu
75 251 PARIS Cedex 05

Pour échanger expériences et réflexions à propos de

l'histoire et l'enseignement des mathématiques

M.: *Mathématiques*
A. *Approche par les*
T. *Textes*
H. *Historiques*

Résumé

Ce numéro 17 de Mnémosyne propose la reproduction d'un article d'Eugène Carissan présentant une machine à factoriser.

L'étude centrale est d'ailleurs consacrée à la factorisation des grands nombres, de Fermat à nos jours.

Le conte du lundi s'intéresse aux codes secrets et propose également des activites en classe sur ce thème.

La rubrique " dans nos classes " étudie un texte de Fermat sur la factorisation.

Mots-clés

Histoire des mathématiques

Fermat, Carissan, Turing

Arithmétique, factorisation, cryptographie, congruences, codes secrets

En vente au prix de 5,00 Euros

Editeur : IREM
Directeur responsable de la publication : M. ARTIGUE
Dépôt légal : Juin 2002
ISBN : 2-88612-223-2
IREM Université Paris VII Denis Diderot
Case 7018
2, place Jussieu 75 251 Paris Cedex 05
Tel : 01 44 27 53 83