CRYPTOGRAPHIE ET THÉORIE DES NOMBRES : QUELQUES REMARQUES SUR LA MÉMOIRE D'UNE RENCONTRE

Catherine GOLDSTEIN

Le codage de messages afin qu'ils ne soient pas lus par des indésirables est attesté depuis plusieurs millénaires. Le développement spécifique de mathématiques complexes pour effectuer ces codages, la mise en place de formations universitaires entièrement orientées sur la cryptographie, en revanche, n'ont que quelques décennies. Cette double chronologie rend particulièrement difficile de comprendre les dynamiques en jeu dans l'établissement de la cryptologie[1] mathématique comme discipline propre. Certains phénomènes peuvent être étirés sur le long terme, comme l'usage politique du domaine ou même le recours à des mathématiques discrètes. D'autres sont souvent décrits comme de radicales innovations, comme les liens entre mathématiciens, militaires et industriels indissociables de la cryptographie contemporaine. Les nombres premiers sont définis et étudiés dans les *Eléments* d'Euclide, c. 300 avant notre ère, mais, comme bien d'autres, Ronald Rivest (le R. du système RSA) attribue[2] à William S. Jevons d'avoir lancé le premier défi de factorisation (trouver deux nombres dont le produit soit 8616460799), en 1874. Ces temporalités sont-elles effectives ou créées par une historiographie plus ou moins spontanée des principaux acteurs du domaine —une historiographie qui, parfois, identifie rétrospectivement des approches modernes dans les processus anciens de codage, ou, au contraire, ignore des configurations lointaines entre sciences et pouvoirs économiques, politiques et militaires parce que la mémoire sociale des mathématiques n'a pas retenu l'importance des domaines pratiques avant le 19e siècle ? « Comment une spécialité qui n'a pas vingt ans d'âge », demande Jacques Stern en 1998, peut-elle revendiquer une histoire de plus de vingt siècles[3] ? ».

QU'EST-CE QU'UNE DISCIPLINE ?

L'impression dominante en assistant actuellement à une conférence sur l'histoire de la cryptographie est bien celle d'une discipline toute juste constituée, ou même en voie de le faire. Or, la notion de discipline, le problème de la disciplinarisation, ont beaucoup intéressé les sociologues et les historiens des sciences. Il faut toutefois noter la variété de leurs définitions de ce qu'est une discipline, de leurs descriptions, et par conséquent des techniques proposées pour les étudier. Certains auteurs mettent l'accent sur l'enseignement : c'est alors avant tout par les manuels, par les programmes de formation spécifiques, que se définit une discipline. Rudolf Stichweh ouvre ainsi son étude fondamentale sur la genèse du système scientifique moderne :

---

[1] Si de nombreux spécialistes distinguent « cryptographie », « cryptologie », « codage », « cryptanalyse », etc., le sens de ces distinctions n'est pas toujours fixé. De plus, ces distinctions ne sont en général pas maintenues dans les classements bibliographiques, comme nous le verrons. J'ai pris le parti ici de les ignorer.

[2] Dans son exposé donné le 8 février 2011, à l'occasion du Killian award, « The growth of cryptography » ; http://people.csail.mit.edu/rivest/pubs/Riv11a.slides.pdf.

[3] J. Stern, *La science du secret*, p. 8.

> « Depuis Aristote, le philosophe a pour tâche de répartir la totalité du savoir humain de manière à dégager un ordre rationnel de la série et de la hiérarchie des domaines du savoir et à rendre possible un passage réglé de l'un à l'autre. Il est manifeste qu'une telle entreprise est liée à la question de l'enseignement scolaire ; de fait, on appelle « disciplines « les unités qu'engendre la classification : il s'agit d'un savoir présenté sous une forme qui peut s'enseigner. Les principes de classification varient avec la forme que prend l'institutionalisation sociale de l'éducation[4]. »

D'autres auteurs, se focalisant sur l'établissement d'un domaine de recherche, identifient une discipline par un ensemble de caractéristiques communes qu'ils repèrent dans les articles ou mémoires de recherche, des textes de synthèse, des rapports. Martin Guntau et Hubert Laitko voient une discipline scientifique comme un « système d'activités orientées-objet » (*object-oriented system of scientific activities*) et non comme un simple système de connaissances. S'appuyant sur leurs travaux, Ralf Haubrich[5] a proposé une liste de composantes permettant de définir une discipline mathématique particulière qui aurait émergé à partir des *Disquisitiones arithmeticae* de C. F. Gauss, et d'identifier, au moins en moyenne, si des travaux particuliers en relèvent : la définition du sujet (les relations entre nombres entiers) ; les concepts clés (congruences et formes quadratiques) et les problèmes associés (la classification poussée des formes en classes, ordre, genre, par exemple) ; l'organisation systémique, reflétée par les classifications des journaux ou les tables des matières des ouvrages de synthèse, comme le *Report on the Theory of Numbers* de H. J. S. Smith pour la British Association for the Advancement of Science, ou l'article « Numbers, Theory of » de la IXe édition de l'*Encyclopaedia Britannica*. On pourrait selon les cas ajouter d'autres critères, comme les modes de preuve acceptés, ou encore les valeurs mises en avant pour apprécier une solution, comme sa généralité, ou le fait qu'elle soit effective.

Si le mot « activités » (dans « système d'activités orientées-objet ») permet en principe d'attacher ce repérage à des pratiques — celles qui forgent définitions et concepts, celles qui classent, ordonnent et diffusent les résultats —, le fait de concevoir une discipline comme orientée vers un objet (de savoir) retentit donc ici sur la nature des critères retenus, internes aux mathématiques.

Plusieurs sociologues, au contraire, ont focalisé leur définition d'une discipline sur l'existence même de la communauté qui la produit. C'est alors à partir du comportement de cette communauté, de ses modes de recrutement ou d'intégration, de ses rites, de ses liens, de ses actions, que la discipline se construit. Colloques ou séminaires spécifiques, lieux particuliers de rencontres ou de publication, postes clés, protocoles partagés, mais aussi, au niveau textuel, réseaux de citations partagées, références croisées, histoires communes répétées, deviennent alors les indices d'une coagulation disciplinaire. Pour Thomas Kuhn,

> « A scientific community consists … of the practitioners of a scientific specialty. To an extent unparalleled in most other fields, they have undergone similar educations and professionzl initiations; in the process the have absorbed the same technical literature and drawn many of the same lessons from it. […] One may usefully ask : What do its membres share that accounts for the relative fulness of their professional communication and the relative unanimity of their professional judgments ? […] I suggest 'disciplinary matrix': 'disciplinary' because it refers to the common possession of the practioners of a particular discipline; 'matrix' because it is composed of ordered elements of various sorts, each requiring further specification[6]. »

Des modèles sociologiques distincts de la construction sociale des sciences ont donné lieu à de nombreuses variantes, qui se traduisent d'ailleurs par des variations ou des dédoublements de vocabulaire ; les mots « champ de recherche » ou « école » ou « community » peuvent par exemple se substituer au mot « discipline » pour décrire des structures de recherche. Le mot

---

[4] Stichweh, *Études* ..., p. 15.

[5] R. Haubrich, « Gaussian Number Theory vs Algebraic Number Theory », Talk at the Conference for the 200 th Anniversary of C. F. Gauss's *Disquisitiones arithmeticae*, Oberwolfach, 2001.

[6] T. Kuhn, *The Structure*..., Postscript, p. 177 et p. 182.

« discipline » peut être selon le cas abandonné, relégué en adjectif (la « matrice disciplinaire » de Kuhn), ou réservé en complément pour le classement institutionnel des enseignements[7].

La cryptographie comme discipline en formation

La plupart des auteurs de ces théories sociologiques se sont aussi intéressés aux mécanismes de la (trans)formation disciplinaire, et plusieurs des phénomènes qu'ils repèrent sont bien à l'œuvre pour la cryptographie. Les témoignages des spécialistes, les présentations des colloques, les préfaces des livres, évoquent ainsi un amalgame de plusieurs courants de recherche relevant de disciplines plus anciennes, et leur recomposition autour de thèmes et de questions clés.

En même temps, les chercheurs concernés commencent à constituer une mémoire collective, à partir tant d'histoires partielles de chacune des composantes que d'épisodes variés de leur rapprochement. Les actes d'un Workshop on Cryptography, à Burg Feuerstein au printemps 1982, se mettent ainsi sous un double patronage : celui du Goethe de « Lust am Geheimnis » et celui du lieu même du colloque, construit au début des années 1940 comme « a camouflaged center for communications engineering emphasizing cryptographic research »[8]. Ce phénomène mémoriel est souvent analysé par les sociologues comme caractéristique de la mise en place d'une nouvelle discipline ou d'un nouveau champ de recherche scientifique.

Une histoire commune du passé s'ajuste ainsi par des négociations sur les acteurs principaux, des anecdotes personnelles, mais partagées, des discussions sur la date exacte d'un événement — séance décisive de séminaire, premier colloque fondateur, cours dans une université, ou publication d'une modélisation particulièrement fructueuse, d'un théorème identifié comme fondamental. Beaucoup de récits adoptent une description globale similaire, opposant une phase de résultats élémentaires, isolés et dispersés, à l'élaboration récente de théories plus mures, fondées sur des outils mathématiques avancés et en interaction fructueuse avec plusieurs domaines. Elwyn Berlekamp, dans un recueil destiné à commémoirer le 25e anniversaire de l'article fondateur de Shannon, écrit ainsi :

> « In the early years of coding theory, nearly all of the interaction with other academic disciplines consisted of discoveries that various minor problems in coding theory could be solved by the application of elementary techniques from other fields. However, in the past decade, coding theroy has matured. Not only has coding theory found applications for a number of deep results in pure mathematics, including the Davenport-Hasse theorem, Weyl's proof of the Riemann hypothesis for function fields, and Baker's recent Field-medal-winning results on Diophantine analysis, but coding theory has also been able to make significant contributions to other areas[9]. »

La structure de ces récits concorde avec d'autres récits de formation disciplinaire, adoptant un schéma analogue[10]. Mais elle cache à peine une grande variété dans les domaines appelés à témoigner, les résultats mentionnés, la chronologie. Berlekamp souligne lui-même la variabilité dans le temps de l'importance historique (*historical significance*) qui peut être accordé à un article

---

[7] Je renvoie à S. Gauthier, *La Géométrie des nombres*…, en particulier pp. 20-24 pour une discussion d'exemples de ces notions en histoire des sciences. Remarquons que ces notions ne coïncident pas a priori, voir C. Goldstein & N. Schappacher, « A Book in Search...» et « Several Disciplines... » pour une illustration de la différence entre « champ de recherches » et « discipline » appliqués à la théorie des nombres.

[8] T. Beth (ed.), *Cryptography…*, citation de Goethe (extraite de la section « Lust am Geheimnis» (Plaisir du secret) du *Traité des couleurs*) en page de garde, et préface respectivement. Plusieurs dispositifs mécaniques de chiffrement, machine Kryha, Enigma, etc., présentées au centre de Burg Feuerstein, sont aussi illustrées dans la partie historique des actes, voir par exemple pp. 6-7.

[9] *ibid.*, p. 1.

[10] Voir par exemple la description que David Hilbert donne en 1896 de la disciplinarisation de la théorie des nombres (en tant que théorie des corps de nombres algébriques) au début du *Zahlbericht*. Ce point est commenté dans C. Goldstein & N. Schappacher, « Several disciplines …», pp. 88-90.

dans ce domaine, selon les travaux que cet article a suscités à une certaine date[11]. L'ère moderne de la cryptographie commence-t-elle avec Shannon, par exemple, ou avec Diffie et Hellman, qui définirent en 1976 le concept de clé publique, annonçant même « l'aube d'une révolution en cryptographie[12] ».

Face à ces constructions mémorielles, stéréotypées dans leur forme mais variables dans leur contenu, la position de l'historienne est un peu celle d'un paléontologue habitué à étudier des collections de petits morceaux fossilisés et qui serait projeté au milieu d'un troupeau de brachiosaures vivants : de (trop) nombreuses informations disponibles, de toute nature, sur toutes sortes de supports, à la fois hétérogènes et parcellaires, rendent difficile une appréciation d'ensemble des mécanismes en jeu dans ce domaine en pleine expansion.

Que peut-on voir en changeant la focale et en se plaçant à une échelle plus grossière, celles des classifications par sujets adoptées par les mathématiciens eux-mêmes ? Depuis le milieu du 19e siècle au moins (avec l'apparition du journal de recension, *Jahrbuch für die Fortschritte der Mathematik*) ces classifications, évolutives dans le temps, permettent de repérer certaines évolutions disciplinaires[13]. Qu'en est-il, par exemple, du standard MSC (*Mathematics Subject Classification*) — schéma de classification international adopté pour localiser tous les articles de mathématiques ? « Cryptography » apparaît dans le titre de 4 rubriques du dernier classement MSC, celui de 2010 :

11T71 : Algebraic coding theory; **cryptography**
14G50 : Applications to coding theory and **cryptography**
81P94 : Quantum **cryptography**
94A60 : **Cryptography**

La première rubrique relève de la section 11, « Théorie des nombres » (plus particulièrement, de « aspects arithmétiques des corps finis »), la deuxième de 14, « Géométrie algébrique » (plus particulièrement « Géométrie diophantienne »), la troisième de 81, « Théorie quantique », la dernière enfin de la section « Communication, Information, Circuits ». Un jeu de renvois[14] pointe aussi sur la rubrique 68P25, « Cryptage de données » (*Data encryption*) de la section Informatique (*Computer Science*) — dont dépend aussi la rubrique 68P30, « Codage et théorie de l'information»— et sur plusieurs rubriques de la sous-section 94B, «Théorie des codes correcteurs » (*Theory of error-correcting codes and error-detecting codes*). Nous sommes d'ailleurs loin d'épuiser ainsi tous les articles pertinents : une recherche sur l'expression « Boolean functions » dans le titre de l'article renvoie, en contexte cryptographique, aux rubriques 94C10, 68T05, 68Q17 etc. L'article fondateur de Richard W. Hamming, « Error detecting and error correcting codes » était recensé en « probabilités » et, plus encore, 13 des 44 classiques sélectionnés par Berlekamp dans son Source book n'ont pas été recensés dans les *Mathematical Reviews*[15].

---

[11] E. Berlekamp, *Key Papers*…, p. 3.

[12] Extrait de leur article « New Directions in Cryptography », cité d'après Jacques Stern, *La science du secret*, p. 85, qui en fait le point de départ du troisième âge de la cryptographie, celui dans lequel nous sommes.

[13] Ainsi que des priorités multiples, liés à une nation, un domaine particulier, un parti-pris méthodologique. On pourra se reporter en particulier à R.Siegmund-Schultze, *Mathematische Berichterstattung…,* et à L.Rollet & P. Nabonnand, « An Answer to the Growth »… pour deux discussions de deux classifications concurrentes au 19e siècle.Voir aussi C. Goldstein et N. Schappacher, « Several Disciplines...», p. 93-96, pour ce que ces classifications reflètent de l'état d'un champ. Rappelons que la MSC est maintenant une norme internationale, utilisée par les deux principaux journaux de recension, *Mathematical Reviews* et *Zentralblatt.*

[14] Ces renvois varient beaucoup, suggérant d'intéressantes micro-réorganisations, par exemple la classification de 2000 met en avant la rubrique 68Q05, Machines de Turing et autres modèles de calcul.

[15] Voit E. R. Berlekamp, *Key Papers*... A quatre exceptions près, les autres articles — ils sont tous antérieurs à 1973 — sont recensés dans la section 94, celle d'informatique.

Cette répartition permet déjà de constater certaines évolutions. Si 94 remonte aux origines des *Mathematical Reviews*, 94A, « Communication, information », est une rubrique datant seulement de 1980, même si elle hérite de rubriques antérieures (dont *Coding Theory* présente entre 1973 et 1979) ; 94A60, en particulier, ainsi que 94B datent aussi de 1980. Il en est de même de 11 T71, présente dès l'apparition de la section 11 (qui remplace alors l'ancienne section 10 consacrée à la théorie des nombres jusqu'alors). Si *Computer Science* est présente dès 1940, la sous-section 68P, *Theory of data*, et en particulier 68P25, datent aussi de 1980 ; notons en revanche que 68P30, *Coding and information theory*, est plus récente, n'apparaissant qu'en 2000. Le lien à la géométrie algébrique ne bénéficie d'une rubrique spécifique, 14G50, qu'en 2000, quant à 81P94, elle vient tout juste d'apparaître, en 2010.

La répartition des articles dans ces rubriques est par ailleurs tout à fait inégale. Depuis 1980, plus de 7000 articles ont 94A60 comme code de classification principal, 7720 ont 94Bx, contre seulement 316 items en rubrique principale 11T71. La plus récente rubrique 14G50 est principale pour 195 articles, alors que 81P94 l'est déjà pour 122. Toutes les rubriques, en revanche, témoignent d'une augmentation importante des publications dans la dernière décennie. La rubrique 94A60 augmente d'un facteur 3,4 entre les années 1990 et les années 2000 (1264 items recensés entre 1990 et 1999, 4380 entre 2000 et 2009), alors que les sections 94B et 11T71, à deux échelles différentes, augmentent d'un facteur 1,5. Structurer ces données, par pays, par lieux de publications (le rôle des IEEE Transactions on Information Theory a été maintes fois souligné) ou par séries (comme celle des actes des colloques Eurocrypt, dans la suite de celui de Burg Feuerstern), par les attaches institutionnelles des auteurs, mais aussi en suivant les liens internes de renvois bibliographiques, de thèmes, de méthodes, d'applications réciproques, à l'intérieur des mathématiques ou à d'autres terrains, serait nécessaire pour une approche sociologique plus sérieuse de l'avènement d'une discipline mathématique associée à la cryptographie[16]. Je me contenterai de noter l'entrelacs des rubriques dans les références croisées, suggestif d'une circulation importante à l'intérieur d'une thématique globale « cryptographie » au-delà des divisions de MSC. L'article fondateur de RSA, classé en 94A05, est en référence de 124 items dans la base des *Mathematical Reviews* : 70 environ relèvent encore principalement de la sous-section 94A (dont 57 en 94A60), une vingtaine de théorie des nombres (dont moins d'une dizaine en code 11T71 principal ou secondaire). L'article le plus ancien recensé en 11T71 apparaît 79 fois en référence dans la base, dont une seule fois pour un article de même code principal.

Les catalogues de bibliothèques peuvent fournir quelques indications supplémentaires (je n'évoquerai ici que la situation en France). La bibliothèque MIR (Mathématiques Informatique recherche) des universités Pierre et Marie Curie et Paris Diderot par exemple propose environ 500 ouvrages pour le sujet « cryptographie/cryptologie ». Les deux plus anciens sont *Cryptography: the science of secret writing*, de Laurence Dwight Smith (écrit en 1943, mais acquis dans l'édition de Dover de 1955) et *Cryptanalysis: a study of ciphers and their solution* de Hélène Fouché Gaines (1956). Les deux ouvrages sont mathématiquement peu techniques et ont été classés dans la section de la bibliothèque sur les recréations mathématiques. Viennent ensuite chronologiquement quelques ouvrages de la fin des années 60, comme l'ouvrage de Berlekamp, *Algebraic Coding Theory* (1968) ou *Elementary Cryptanalysis: a mathematical approach*, d'Abraham Sinkov, incluant des programmes de Paul Irwin (1966). Ces livres comprennent entre autres des chapitres sur les corps finis ; or, ils sont situés (selon leur mode d'acquisition) dans la partie informatique de la bibliothèque. A partir des années 80, le nombre de titres croit nettement et leur localisation se diversifie (reproduisant en partie la répartition perçue par MSC). La même recherche sur les

[16] Pour des exemples de cette démarche, appliquée à la théorie des nombres, voir C. Goldstein & N.Schppacher, « A Book in Search… » et « Several Disciplines… », et S. Gauthier, *La Géométrie des nombres*....

bibliothèques de l'ENS produit 75 titres, principalement classés en informatique, mais aussi une vingtaine d'ouvrages dans la bibliothèque de lettres, liés soit à des ouvrages historiques sur le chiffre militaire et les langages cryptés à différentes périodes, soit au déchiffrement des langues. Sur une plus longue durée, une recherche analogue sur la base Sudoc donne 1250 ouvrages dont le plus ancien (les six livres de polygraphie de Triphème, en latin) remonte au 16e siècle, le mot « cryptographie » apparaissant couramment dans les titres au 19e siècle ; il est alors lié au déchiffrement de toutes sortes d'écritures secrètes et à ses usages, comme dans deux ouvrages de 1893 *De la cryptographie : essai sur les méthodes de déchiffrement*, de P. L. E. Valerio ou dans la *Cryptographie nouvelle, assurant l'inviolabilité absolue des correspondances chiffrées* de F. Delastelle, amateur maintenant bien connu, également auteur de *Mathématiques appliquées. Traité élémentaire de cryptographie* en 1902. La localisation de ces ouvrages est significative : jusqu'à la deuxième guerre mondiale, ils sont hébergés principalement à la Bibliothèque Sainte-Geneviève, à la Bibliothèque nationale ou, pour ceux rédigés par des militaires, au CNAM, ce qui les situe alors hors du strict monde académique, incarné par la Faculté des sciences. Les bibliothèques des universités de province en ont peu avant une époque très récente — certains fonds témoignant de la forte institutionnalisation de ces sujets dans les années 1990.

Cette enquête superficielle fait donc apparaître la complexité d'une histoire disciplinaire de la cryptographie. Si la multiplicité des professions en jeu a déjà bien été repérée, nous voyons ici que les liens concrets avec les mathématiques ne relèvent pas d'une simple dynamique progressive de transfert de connaissances, des mathématiques pures vers des applications que l'informatique serait venue renforcer. Qu'une bibliothèque d'informatique héberge les livres de mathématiques orientés vers le codage avant que le sujet ne réintègre les bibliothèques de recherche en mathématiques suggère une dynamique d'appropriation préalable par une communauté nouvelle ; la coupure dans l'héritage des recréations mathématiques mériterait aussi un examen détaillé — rappelons que c'est dans ce cadre contraint qu'Edouard Lucas a à la fin du 19e siècle construisit un environnement mathématique adéquat pour le jeu de Nim ou le baguenaudier (codes de Gray), ou que Martin Gardner donna un large retentissement au système RSA en 1977 via sa colonne de jeux dans *Scientific American*. Du même coup, s'explique la difficulté de mettre en place une mémoire collective commune : selon les rencontres, les opportunités, c'est l'appropriation d'un outil différent, d'un élément particulier qui apparaîtra comme décisif, et c'est l'histoire de cet élément de contact, redéployée vers le passé, qui sera décrite. Plusieurs caractérisations du domaine, insistant sur des aspects différents, ont ainsi été suggérées : la mécanisation des calculs, l'importance attachée à l'effectivité dans des domaines de mathématiques pures jusqu'alors, comme la théorie des nombres ou la géométrie algébrique ; une attention spécifique au temps, temps humain, temps d'exécution d'une tâche ; des questions autour de l'aléa, du probable, des degrés de sécurité ; la réflexion sur le langage, au (dé)chiffrement, à la combinatoire des signes ; les liens entre art de la guerre, mathématiques, industrie et pouvoirs politiques, liens de résultats et de méthodes, liens de personnes aussi. Or, de telles configurations, du point de vue des éléments qui les composent, ne sont pas propres à la période contemporaine. Il peut donc être utile de les désenclaver de l'histoire stricte de la cryptographie dans l'espoir de mieux mettre à jour quels aspects les attachent spécifiquement à cette histoire. Je me contenterai d'illustrer cette suggestion à partir de quelques exemples de résultats récents portant sur l'histoire de la théorie des nombres.

Nombres, temps, langages, machines au 17e siècle

Il est banal, dans le cadre d'une histoire de la cryptographie, de repérer des travaux mathématiques pertinents dès le 17e siècle. Ceux de Pierre Fermat, en particulier, puisque le petit

théorème de Fermat[17] est au cœur de l'algorithme RSA. L'énoncé apparaît bien explicitement dans sa forme forte sous la plume de l'auteur éponyme. Dans une lettre du 18 octobre 1640, Fermat écrit ainsi :

> « Tout nombre premier mesure infailliblement une des puissances -1 de quelque progression que ce soit, et l'exposant de la dite puissance est sous-multiple du nombre premier -1; et après qu'on a trouvé la première puissance qui satisfait à la question, toutes celles dont les exposants sont multiples de l'exposant de la première satisfont tout de même à la question.
> Exemple : soit la progression donnée
> 1 2 3 4 5 6
> 3 9 27 81 243 729 etc.
> avec ses exposants en dessus. Prenez par exemple le nombre premier 13. Il mesure la troisième puissance -1 de laquelle 3, exposant, est sous-multiple de 12, qui est moindre de l'unité que le nombre 13, et parce que l'exposant de 729, qui est 6, est multiple du premier exposant, qui est 3, il s'ensuit que 13 mesure aussi la dite puissance 729-1.[18] »

Ce résultat exprime pour nous que le groupe multiplicatif du corps fini $\mathbf{F}_p$ est cyclique, d'ordre *p-1*. En tant qu'élément de l'histoire de la cryptographie, la mention de ce théorème illustre en général l'idée que des mathématiques élaborées depuis longtemps pour elles mêmes, de manière purement théorique, se trouvent utilisables dans des contextes appliqués.

Pourtant, le (petit) théorème de Fermat n'est pas originellement un résultat structurel, valorisé en tant que tel. L'objectif de Fermat est d'étudier la divisibilité par différents nombres premiers de suites de la forme a^n-1, a fixé (« une des puissances -1 de quelque progression que ce soit » — Fermat oubliant de préciser dans sa lettre que ces nombres premiers ne doivent pas diviser a). Il énonce donc ici qu'il existe toujours des exposants n pour lequel cette divisibilité a lieu (« Tout nombre premier mesure infailliblement une des puissances -1»), et que le plus petit de ces exposants est un diviseur (un « sous-multiple ») de *p-1*. En termes actuels, il s'agit bien de déterminer l'ordre de a dans le groupe multiplicatif (cyclique) de $\mathbf{F}_p^*$, mais pour Fermat, a est fixé, p varie. Cette différence de perspective est liée à la finalité de son résultat : il s'agit de raccourcir les calculs dans la recherche des nombres parfaits, c'est-à-dire égaux à la somme de leurs diviseurs propres, et plus généralement dans la recherche des nombres qui ont un rapport donné à la somme de leurs diviseurs propres. Comme maintenant, les nombres parfaits connus à l'époque de Fermat, en application directe d'un théorème des *Eléments* d'Euclide, étaient ceux de la forme $2^{n-1}(2^n-1)$, avec 2^n-1 est premier. Ceci implique d'examiner les diviseurs possibles de 2^n-1 (et plus généralement de a^n-1). L'emploi de son théorème permet à Fermat de fabriquer des nombres très grands sous-multiples de leur somme de diviseurs propres, comme 1 802 582 780 370 364 661 760 (qui vaut le quart de la somme de ses diviseurs propres), ou de s'assurer qu'il n'y a pas de nombres parfaits à 20 ou 21 chiffres[19] ; en liant diviseurs premiers possibles et exposants, il élimine en effet d'office la plupart des nombres premiers comme diviseurs. La nécessité d'améliorer la recherche des facteurs premiers est clairement exprimée : Fermat se plaint des « fréquentes divisions qu'il faut faire pour trouver les nombres premiers », loue particulièrement un des correspondants sur ces questions, Bernard Frenicle de Bessy, pour « la vitesse de ses opérations », propose sa méthode pour déterminer plus efficacement si un nombre est composé, par différence de carrés[20].

---

[17] Il s'agit du fait que, si p est un nombre premier et a un entier premier à p, alors $a^{p-1} \equiv 1 \bmod p$ (c'est-à-dire que p divise $a^{p-1}-1$). La notation actuelle utilisée ici (« ≡ ») remonte aux *Disquisitiones arithmeticae* de C.F. Gauss, en 1801.

[18] P. Fermat, *Correspondance...*, p. 209.

[19] *ibid*., p. 248, p. 194 et p. 210, resp.

[20] *ibid.*, p. 187 et p. 257.

L'intérêt pour ces questions n'est pas propre à Fermat, et relève bien d'enjeux collectifs[21]. Ceux-ci sont régulièrement évoqués dans les écrits, correspondances ou mémoires du cercle de Marin Mersenne (auquel appartient Frenicle et dont Fermat est correspondant), et frôlent l'histoire de la cryptologie de multiples façons. Témoin les procédures mises en place pour contourner le manque de confiance dans la transmission scientifique à distance, comme celle d'échanger problèmes et solutions numériques, en lieu des méthodes ou des règles générales. Témoin, encore, l'intégration du temps dans l'*énoncé même des problèmes*. Voici par exemple la demande que reçoit Fermat de ce cercle, en avril 1643 :

> « Vous me demandiez ensuite si [100 895 598 169] est premier ou non, et une méthode pour découvrir dans l'espace d'un jour s'il est premier ou composé[22]. »

Il y a donc dans ce milieu temps imposé — même si ce temps peut nous sembler long et qu'il n'y ait pas de trace dans ces lettres d'une véritable évaluation quantitative de ce temps — et prise de conscience des problèmes spécifiques liés à la taille des nombres en jeu.

Marin Mersenne et les membres de son entourage s'intéressent de près au problème des langues artificielles et à celui des chiffres, souvent perçus comme analogues[23]. Leurs correspondances, leurs ouvrages évoquent tant Jérôme Cardan que Blaise de Vigenère, ou bien sûr François Viète. En lien avec des problèmes de combinatoire, Mersenne a proposé dans son *Harmonie universelle* un moyen d'« escrire toutes sortes de lettres secrettes », soulignant l'utilité de son ouvrage pour les affaires de l'Etat. Un proche de Mersenne, Aimé de Gaignières, défie Antoine Rossignol, cryptologue professionnel au service de l'Etat, et tant Frenicle que Mersenne deviennent attentifs au fait que les deux opérations de chiffrer et de déchiffrer ne sont pas inverses l'une de l'autre de manière transparente. Frenicle dit ainsi dans son *Abrégé des combinaisons*, composé vers 1640, et publié à la fin du siècle :

> « Mais ce n'est pas assez de sçavoir écrire, si l'on se sçait lire son écriture, & ce n'est pas peu de chose que de sçavoir lire celle-ci : car ceux mêmes qui l'auroient écrite ne la pourroient lire, s'ils n'en sçavaient la méthode, quoiqu'ils sçussent celle de l'écrire[24]. »

L'élaboration d'instruments et de machines aptes à implémenter ces combinatoires de signes est aussi à l'ordre du jour. C'est le fils d'un autre proche de Mersenne, et lui-même inséré jeune dans son cercle, Blaise Pascal, qui concevra d'ailleurs une machine arithmétique commercialisée — et, rappelons-le, bénéficiera d'un privilège royal sur toute la production.

Nous trouvons donc dès le 17e siècle non seulement les quelques éléments éparpillés usuels dans toute histoire de la cryptologie — le petit théorème de Fermat, un ou deux cryptologues proches du pouvoir royal, comme les Rossignol — mais une configuration, tant épistémique que sociale, qui inclut un intérêt pour le chiffrement et le déchiffrement, une appréciation de ses enjeux politiques, une réflexion sur leurs liens complexes et sur la calculabilité, la construction de machines variées, des mathématiques liées à la combinatoire et à la primalité.

INDUSTRIE, ORDINATEURS ET THÉORIE DES NOMBRES

Qu'en est-il maintenant de la suggestion qu'ordinateurs et potentialités industrielles ont été les facteurs décisifs pour l'avénement de la cryptologie ? Le fait est que leurs routes croisent la théorie

---

[21] Sur ces enjeux, et en particulier le rôle de la taille des nombres et du temps dans les questions mathématiques de ce milieu, voir C. Goldstein, « L'arithmétique de Fermat… ».

[22] *ibid*., p. 255. Le nombre est composé, produit de 898 423 et 112 303.

[23] Ces relations et leurs liens avec les mathématiques sont examinées dans la thèse d'Ernest Coumet, *Mersenne, Frenicle*... ainsi que dans son article « Cryptographie…».

[24] Cité dans E. Coumet, « Cryptographie…», p. 1021. L'histoire de la cryptographie, tout en soulignant l'importance de ces questions, ne retient d'ordinaire que Rossignol, voir D. Kahn, *The Codebreakers*, ch. IV et V.

des nombres bien avant les années 1980. Comme l'a bien montré Anne-Marie Décaillot[25], Edouard Lucas combine à cet égard bien des atouts, dès la seconde moitié du 19e siècle. Il s'intéresse explicitement à la cryptographie, il est en contact avec les milieux industriels, son travail de recherche concerne en priorité combinatoire et arithmétique. Plus spécifiquement, il examine la réciproque du théorème de Fermat, dans la perspective de tests de primalité : le fait que (**Z**/n**Z**)* soit cyclique d'ordre n-1 caractérise les entiers n premiers, autrement dit *n* est premier si et seulement s'il existe un entier *a* (<*n*) tel que *n* divise $a^{n-1} - 1$, mais en revanche ne divise aucun des nombres $a^{(n-1)/q} - 1$, pour $q>1$ diviseur premier de $n-1$. La mécanisation de tests de primalité ne lui était d'ailleurs pas étrangère, même si la machine qu'il imagine ne nous est pas parvenue. Lucas a aussi relancé les études mathématiques de problèmes situés dans le cadre des recréations mathématiques, mais faisant apparaître de la complexité, comme les tours de Hanoi. Mais un point remarquable de sa situation est sa tentative d'appliquer ses recherches arithmétiques à des situations industrielles ; comme en témoignent les comptes rendus de l'Association française pour l'avancement des sciences, il n'est ici pas isolé, même s'il est sans doute le plus célèbre à s'engager dans ces interfaces. Dans le cas de Lucas, l'industrie est textile, et il s'agit donc, non de sécurité de transmission, mais de modélisation et mécanisation du tissage, des satins en particulier, par l'arithmétique modulaire.

Le passage à l'ordinateur ne semble d'ailleurs pas modifier radicalement ces configurations, dans lesquels de nombreux éléments que nous associons maintenant à l'avénement de la cryptographie sont en place, mais reliés de manière différente. C'est d'ailleurs par des machines, cribles électriques, engrenages empruntés à des vélos, que les Lehmer, Derrick Norman et son fils Derrick Henry, ont d'abord poursuivi leurs investigations sur les nombres premiers dans la lignée de Lucas (le père factorisant en 1903 le nombre de Jevons, 8616460799, auquel nous avons fait allusion au début de cet article). La crise économique des années 30 qui contribue à lancer D. H. Lehmer et son épouse Emma, également mathématicienne, dans divers périples à la recherche de postes, et du même coup favorise leurs nombreux contacts ; la seconde guerre mondiale, qui donne à Lehmer l'occasion de lancer un programme plus ambitieux avec des ordinateurs puissants ; la concurrence entre universités aux USA, sont autant de facteurs importants dans la création de l'Institute for numerical analysis et le rôle des Lehmer dans ses orientations : le SWAC (Standard Western Automatic Computer) en est une des retombées cruciales[26]. Cet ordinateur très puissant pour l'époque soude de nouveaux liens entre universités et industrie : il est utilisé dans l'industrie locale de l'aviation, mais il permet aussi aux Lehmer et à leur équipe, dans l'intervalle des calculs industriels, d'en développer d'autres, orientés vers la théorie des nombres. Pourtant, cet épisode ne témoigne pas d'une exceptionnelle connivence entre mathématiciens professionnels et industriels autour des calculs et des machines, qui serait propre aux Etats-Unis. D'une part, parce que Lehmer insiste alors sur l'aspect désintéressé des mathématiques qu'il pratique, bien plus que sur l'applicabilité éventuelle de ses travaux: « The most compelling urge to the study of mathematics », affirme-t-il en 1932, « is not its practical application to the study of every day, bread-and-butter life, but lies in the romance and glamour surrounding its mysterious secrets[27] ». Il s'agit bien de « week-end off[28] », d'une répartition harmonieuse du temps de calcul des ordinateurs, pas d'un engagement

[25] A.-M. Décaillot, « L'arithméticien Edouard Lucas…».

[26] Voir L. Corry, « FLT meets SWAC...» et « Hunting Prime Numbers...», ainsi que M. Bullynck et L. De Mol, « A week-end off…».

[27] Cité dans L. Corry, « Hunting Prime Numbers...».

[28] M. Bullynck et L. De Mol, « A week-end off…».

systématique des mathématiciens dans les problématiques industrielles. D'autre part, surtout, parce que des rapprochements analogues se retrouvent dans d'autres pays tout au long du 20e siècle.

En France même, la première guerre mondiale a été l'occasion de nouvelles synergies entre universitaires, militaires, industriels —même si par exemple l'intérêt pour l'aviation chez les mathématiciens et une perception de l'avion comme un assemblage de problèmes mathématiques date de la première décennie. L'entre-deux-guerres voit l'arrivée massive d'industriels et de militaires au sein de la Société mathématique de France[29]. A l'inverse, des mathématiciens purs se réorientent après guerre, parfois sous l'effet de leurs activités de guerre, vers des domaines vraiment appliqués. C'est le cas de Jean Kuntzmann qui après sa thèse d'algèbre en 1934 se consacre aux mathématiques de l'ingénieur, puis aux mathématiques de l'informatique, et crée en 1951 le premier laboratoire de calcul à Grenoble. C'est aussi le cas pour Albert Châtelet dont la thèse en 1911 porte sur les matrices appliquées à la théorie des nombres[30]. Servant pendant la première guerre mondiale au Centre d'essais balistiques de Gâvre où il est affecté aux calculs, il est chargé après guerre de la reconstruction de l'université lilloise ; il y sera recteur avant de devenir une personnalité importante de l'éducation nationale dans les années 50, créateur du Crous, et même candidat à l'élection présidentielle de 1958. Avec Paul Dubreil, il lance juste après guerre, en 1947, un séminaire d'algèbre et de théorie des nombres qui fait la part belle aux avancées théoriques de ce domaine considéré comme l'un des plus abstraits des mathématiques (variétés algébriques, théorie des idéaux, théorie des groupes...), mais en même temps, il insiste, contrairement par exemple au groupe contemporain rassemblé sous le nom de Bourbaki, sur l'importance des calculs effectifs, sur les problèmes spécifiques que posent ces calculs et sur l'applicabilité de ces domaines à la physique et à l'industrie. Dans sa propre notice sur travaux, Albert Châtelet établit avec soin des ponts entre ses différents aspects :

> Lorsque le Faculté des sciences de Paris, en octobre 1940, voulut bien me charger de l'enseignement d'Arithmétique supérieure, qu'elle venait de créer, j'ai pu exposer dans mes cours les théories algébriques modernes […] Il y a quelque intérêt à signaler que l'Algèbre abstraite, qui reprenait ainsi droit de cité dans le pays de Galois, de Jordan, d'Hermite et de Henri Poincaré, trouvait en même temps des applications fécondes, non seulement en physique théorique, mais encore dans la technique industrielle[31].

Les travaux de recherche propres de Châtelet, peu nombreux au milieu de ses activités administratives et pédagogiques, ne semblent guère propices à l'ancrer dans une histoire de la cryptographie, même si leurs orientations sur les calculs effectifs, l'usage des matrices, tranchent quelque peu avec les injonctions de l'algèbre structurale, qui privilégie l'intrinsèque et néglige alors les questions d'effectivité. En revanche, il illustre des courants mal connus des mathématiques de l'immédiat après-guerre, dont l'effet sur l'essor de la cryptologie mathématique en France mérite peut-être d'être réévalué. Le séminaire qui s'est poursuivi en deux branches et différents organisateurs (Dubreil-Pisot, Pisot-Delange, Pisot-Delange-Poitou, etc.) a servi de point de ralliement de tendances très variées en théorie des nombres ou en algèbre jusqu'aux années 1990[32]. Notons simplement à titre d'exemple que c'est dans ce séminaire (Dubreil-Pisot) que Marcel-Paul Schützenberger a exposé en 1956 une « Théorie algébrique du codage » ; les travaux de

---

[29] Voir D. Aubin et al., « Les mathématiciens français…».

[30] Voir la biographie de A. Châtelet par J. -F. Condette, *Albert Châtelet…* et sur ses activités de guerre et leurs effets, S. Gauthier, « Albert Châtelet…». Un autre exemple intéressant de la génération suivante est celui de René de Possel, d'abord membre de Bourbaki : s'orientant vers l'analyse numérique et l'informatique, il fut le directeur de l'institut Blaise Pascal du CNRS dans les années 60, voir P. E. Mounier-Kuhn, *L'informatique*....

[31] A. Châtelet, *Notice*…. Je remercie les Archives de l'Académie des sciences de m'avoir permis de consulter et de citer ce document. Châtelet, qui n'avait pas les faveurs du gouvernement de Vichy, prit en fait ses fonctions plus tardivement. Sa candidature, en concurrence avec celle de C. Chevalley, membre fondateur de Bourbaki et mathématicien de premier plan, fit l'objet de polémiques.

[32]

Schützenberger s'inscrivent ainsi au début sous la double influence de Châtelet et Dubreil du côté algébrique (il a suivi le cours de Châtelet sur les treillis et celui-ci est un des trois membres de son jury de thèse en 1953, avec Maurice Fréchet et Georges Darmois) et de Darmois du côté des probabilités.

Rencontres

Cette excursion dans les rencontres de l'arithmétique avec la science du codage met en évidence deux écueils. Le premier serait, n'attrapant du passé que des bribes ponctuelles, pauvres et décontextualisées, de voir à trop bon compte dans les dernières décennies une rupture radicale, qui instaureraient pour la première fois des liens entre théorie des nombres, cryptologie, collectivités multiples, pouvoirs économiques, militaires et politiques. Couper complètement les fils qui relient au 17e siècle le professionnalisme d'un cryptographe comme Rossignol des théorèmes d'un Fermat, pour les insérer dans deux histoires, qui serait l'une celle du secret, l'autre celle des corps finis ; négliger les occasions variées, tout au long du 20e siècle, où calculs arithmétiques et ordinateurs ont réuni autour d'une même machine, dans un même lieu, à un même cours, acteurs oubliés de la politique universitaire et futurs héros de la cryptologie, empêche de comprendre les socs sur lesquels la cryptologie s'est finalement sédimentée. Mais le second écueil serait de diluer complètement dans ce passé enrichi les innovations, la radicalité du changement quantitatif des dernières décennies. En ce sens, la mémoire constituée des cryptologues, pour parcellaire qu'elle soit par rapport à l'historiographie, est elle aussi à prendre au sérieux. L'enrichissement du passé doit plutôt nous aider à dégager les spécificités propres à la configuration actuelle. Par exemple de scruter plus précisément comment le développement d'emplois ou d'autres enjeux économiques nouveaux, liés à une utilisation quotidienne, familière, d'objets techno-mathématiques impliquant la cryptologie, est lié à la mise en place de formations universitaires systématiques et au recrutement de chercheurs dans diverses institutions. Ou à une toute autre échelle, non moins pertinente, de cerner comment le « partage de secret publiquement vérifiable » peut être utilisé dans la description de l'organisation des échanges mathématiques au 17e siècle, mais, au 21e siècle, être devenu en soi un énoncé scientifique.

Bibliographie

Aubin, D., Gispert, H. & Goldstein C., « Les mathématiciens français dans la Grande Guerre », in F. Bouloc, R. Cazals, A. Loez (éd.), *1914-1918. Identités troublées : les appartenances sociales et nationales à l'épreuve de la guerre*, Toulouse, Privat, 2011, p. 183-197.

Berlekamp, E. R. (ed.), *Key Papers in The Development of Coding Theory*, New York, IEEE Press, 1974.

Beth, T. (ed.), *Cryptography. Proceedings of the Workshop on Cryptography Burg Feuerstein, Germany, March 29- April 2, 1982*, Lecture Notes in Computer Science 149, Berlin, Heidelberg, New York, Springer, 1983.

Bullynck, M. & De Mol, E., « A week-end off. The first extensive number-theoretical computation on the ENIAC », in A. Beckmann ; A. Dimitracopoulos et B. Löwe (eds.), *Logic and Theory of Algorithms. Computability in Europe 2008*, LNCS 5028, Heidelberg, Springer, 2008, pp. 158–168.

Châtelet, A., *Notice sur les Titres et Travaux scientifiques*, Paris, s.n., 1953.

Condette, J.-F., *Albert Châtelet. La République par l'école (1883-1960)*, Arras, Artois Presses Université, 2009.

Corry, L., « FLT Meets SWAC: Vandiver, the Lehmers, Computers and Number Theory (1930-1956) », *Annals of the History of Computing* 30 (1) (2008): 38-49

— « Hunting Prime Numbers from Human to Electronic Computers », *The Rutherford Journal - The New Zealand Journal for the History and Philosophy of Science and Technology (rutherfordjournal.org)*, 3 (2010).

Coumet, E., *Mersenne, Frenicle et l'élaboration de l'analyse combinatoire dans la première moitié du XVIIe siècle*, Thèse de 3e cycle, 1968.

— « Cryptographie et numération », *Annales. Economies, Sociétés, Civilisations* 30 (1975), pp. 1007-1027.

Décaillot, A.-M., « L'arithméticien Edouard Lucas (1842-1891) : Théorie et instrumentation », *Revue d'histoire des mathématiques* 4 (1998), pp. 191-236.

Fermat, P., *Correspondance, Oeuvres de Fermat publiées par les soins de MM. Paul Tannery et Charles Henry, tome deuxième*, Paris, Gauthier-Villars, 1894.

Gauthier, S., *La Géométrie des nombres comme discipline (1890-1945)*, Thèse de doctorat de l'UPMC, Paris, 2007, http://math.univ-lyon1.fr/~gauthier/recherche/theseGauthier.pdf

— « Albert Châtelet, de la théorie des nombres à la politique universitaire », in C. Goldstein & D. Aubin, *La Grande Guerre des mathématiciens français*, en préparation.

Goldstein, C., « L'arithmétique de Fermat dans le contexte de la correspondance de Mersenne : une approche micro-sociale », *Annales de la Faculté des sciences de Toulouse* 18, n. spécial, 2009, pp. 25-57.

Goldstein, C. & Schappacher, N., « A Book in Search of a Discipline (1801-1860) » , in Goldstein, C., Schappacher, N., et Schwermer, J. (eds.), *The Shaping of Arithmetic after C. F. Gauss's* Disquisitiones arithmeticae, New York, Berlin, …, Springer, 2007, pp. 3-65.

— « Several Disciplines and a Book (1860-1901) », in Goldstein, C., Schappacher, N., et Schwermer, J. (eds.), *The Shaping of Arithmetic after C. F. Gauss's* Disquisitiones arithmeticae, New York, Berlin, …, Springer, 2007, pp. 66-103.

Guntau, M. & Laitko, H. (dir.), *Der Ursprung der modernen Wissenschaften: Studien zur Entstehung wissenschaftlicher Disziplinen*, Berlin, Akademie Verlag, 1887.

Kahn, D., *The Codebreakers : The Comprehensive History of Secret Communication from Ancient Times to the Internet*, Rev. Sub. Ed., New York, Scribner, 1996.

Kuhn, T., *The Structure of Scientific Revolutions*, Second Edition, Chicago and London, University of Chicago Press, 1970.

Mounier-Kuhn, P. -E., *L'informatique en Frnce de la seconde guerre mondiale au Plan Calcul. L'émergence d'une science*, Paris, PUPS, 2010.

Rivest, R., Shamir, A. & Adleman, L., « A Method for obtaining digital signatures and public-key cryptosystems », *Communications of the ACM* 21-2 (1978), pp.120–126.

Rollet, L. & Nabonnand, P., « An Answer to the Growth of Mathematical Knowledge ? The *Répertoire bibliographique des sciences mathématiques* », *European Mathematical Society Newsletter* 47 (mars 2003), pp. 9-14.

Siegmund-Schultze, R., *Mathematische Berichterstattung in Hitlerdeutschland : der Niedergang des* Jahrbuchs über die Fortschritte der Mathematik, Studien zur Wissenschafts-, sozial- und Bildungsgeschichte der Mathematik 9, Göttingen, Vandenhoeck & Ruprecht, 1993.

Stern, J., *La Science du secret*, Paris, Odile Jacob, 1998.

Stichweh, R., *Études sur la genèse du système scientifique moderne*, trad. F. Blaise, Lille, PUL, 1991.