MATHÉMATIQUES ET SCIENCES HUMAINES

ERNEST COUMET

Un texte du XVIe siècle sur les cadenas à combinaison

Mathématiques et sciences humaines, tome 22 (1968), p. 33-37

<http://www.numdam.org/item?id=MSH_1968__22__33_0>

M.S.H. (6e année, no 22, 1968, p. 33-37)

UN TEXTE DU XVIe SIÈCLE SUR LES CADENAS A COMBINAISON

par

Ernest COUMET

I

• LE MATHÉMATICIEN FACE A LA SERRURE

On peut lire dans le *De Subtilitate* de Cardan, une description de ces cadenas à combinaison dont l'usage est encore courant de nos jours :

« Si ie vouloi ici reciter & nombrer toutes les façons des serrures, la narration engendreroit ennui. Toutefois ie mettrai ici l'exemple d'une que Ianellus a composée.

Ceste serrure sous tout nom qui fut de sept lettres pouvoit exactement estre close & fermee : & ne pouvoit estre ouverte sous autre nom que sous celui dont elle avoit esté fermee... »

Sur chaque côté du montant du cadenas, se trouvent deux petites lignes qui servent de repère :

« A ces lignes sept lettres de diction doivent estre mises droit à droit, en tournant & en adaptant les cercles ou anneaux par l'ordre que tu as proposé de garder : comme ainsi soit que le nom soit de sept lettres SERPENS, chacun anneau constituera sa lettre alendroit de l'espace de deux lignes, à fin qu'elle puisse estre close ou ouverte [...]. Et quand la serrure sera fermee, les anneaus sont tournés sans empeschement, à fin qu'ainsi la proportion du nom soit confondue. » [1]

« Serrure ou cadenat faict en façon esmerveillable », dit un ouvrage de « secrets » où se trouve reproduit le texte de Cardan [2]. Pareille curiosité devait sans nul doute flatter le goût du mystère si répandu au XVIe siècle et que ne devait pas entièrement renier le XVIIe. Mais de Cardan, du moins, on aurait pu espérer, sur ce sujet, quelque notation de mathématicien : d'autant qu'il s'était préoccupé d'analyse combinatoire. Le défi qu'avaient en quelque sorte jeté les artisans à l'esprit de méthode ne resta pas toutefois sans réponse : ces cadenas que l'on doit à la subtilité des faiseurs d'artifice, n'y a-t-il pas moyen de les ouvrir à coup sûr, si l'on sait s'y prendre habilement ?

Telle est la question que s'est posée Jean Borrel (plus connu sous le nom de Butéo, 1492 (?)-1572 (?)) dans sa *Logistica*, ouvrage de mathématiques écrit en latin, et publié à Lyon en 1559 [3]. Le texte [4] dont nous donnons la traduction ci-dessous, et qui fait suite à une brève description du mécanisme des serrures à combinaison, frappe par la fermeté avec laquelle la difficulté se trouve réduite, étapes

---

1. Traduction du *De Subtilitate* par Richard Le Blanc, à Paris, par Guillaume Le Noir, 1556, fol. 336 verso.

2. Jacobus Weckerus, dans une compilation intitulée *De Secretis Libri XII* (Bâle, 1587) avait reproduit (p. 711-713) le texte de Cardan. Cette compilation fut maintes fois rééditée. L'expression que nous citons se trouve dans l'index d'une traduction française, *Les secrets et merveilles de nature*, à Tournon, par Claude Michel, 1606.

3. Dans sa *Logistica*, Jean Borrel tenta de regéométriser les notations et la terminologie algébrique. Tout en critiquant violemment certaines tentatives de quadrature du cercle, il développe par ailleurs une méthode assez curieuse de duplication du cube par approximations successives (*Histoire Générale des Sciences*, publiée sous la direction de R. Taton, tome II, « La Science Moderne », Paris, P.U.F., 1958, p. 44).

4. *Logistica*, p. 314-329.

par étapes : Jean Borrel y explicite clairement avec la patience des initiateurs la méthode *lexicographique* de dénombrement et d'énumération.

Puisqu'aussi bien il en fera mention ci-dessous, précisons qu'avant de s'occuper de cadenas, il avait rencontré, dans la même *Logistica*, à propos de jets de dés, un autre problème de dénombrement et d'énumération : il avait dressé les tables des combinaisons avec répétition de six chiffres pris un à un, deux à deux, trois à trois, quatre à quatre.

II

● LES MOTS ET LES CLAUSES

Traduction du texte de Jean Borrel

Imaginez maintenant, à propos d'un instrument construit selon l'un des modes dont on vient de parler, que quelqu'un, désireux de l'ouvrir, ait oublié la formule ; je pose la question suivante : selon quelle méthode la recherche peut-elle être conduite pour que nous ne soyons pas forcés de briser la serrure ?

Pour découvrir cet endroit déterminé où se fait l'ouverture, il faut, de toute nécessité, établir une table bien ordonnée, dans laquelle sont contenus, sans qu'aucun soit omis, tous les modes de révolution [1], distincts entre eux, qui peuvent se produire lorsqu'on fait tourner quatre anneaux. Comme parmi tous ces modes, il en est un, unique, selon lequel a été obtenue la fermeture, c'est en le retrouvant qu'on provoque en effet l'ouverture. Mais c'est là une tâche à ce point longue et compliquée qu'il faut user, pour construire la table, d'un artifice peu commun. Personne jusqu'ici n'a traité ce sujet. C'est que, comme cela apparaîtra dans ce qui suit, la variation parcourt jusqu'à 1 296 modes. Aussi n'y a-t-il pas lieu de compter sur une découverte fortuite. Car, comme le dit Cicéron dans le *De Divinatione* : « En jetant quatre osselets au hasard, il se peut qu'on obtienne le coup de Vénus [2], mais si l'on en jetait quatre cents obtiendrait-on cent fois ce même coup ?» [3]. Pour mieux faire entendre comment va procéder notre recherche, il faudra en amorcer l'exposé à partir de ses cas les plus simples, c'est-à-dire en considérant le cas d'un anneau unique ; après quoi, il faut passer au cas de deux anneaux, puis à celui de trois, et enfin à celui de quatre. Et bien que les formes gravées sur les anneaux soient celles de lettres, je vous demande toutefois, pour la plus grande commodité de l'exposé, de vous représenter chacun de ces anneaux comme portant non pas des lettres, mais autant de nombres progressant à partir de l'unité, à savoir 1, 2, 3, 4, 5, 6. Il n'est pas nécessaire de conserver l'ordre de la progression. On dira plus loin de quelle manière ces nombres correspondent aux lettres. Mais venons-en à la détermination des tables. Bien que celles-ci aient quelque chose de semblable aux tables relatives aux jets de dés qu'on a vues ci-dessus, elles en diffèrent cependant beaucoup, et leurs dimensions s'accroissent plus vite.

La première table, correspondant au cas d'un seul anneau, sera constituée de six caractères représentant des nombres en progression naturelle, et cette table aura autant de parties qu'il y a de nombres ; elle se présente de cette manière : 1 , 2 , 3 , 4 , 5 , 6. Il est manifeste en effet, que pour un seul anneau, aucune variété de révolution ne peut aller au-delà des six lettres que comporte l'anneau.

Pour deux anneaux, on obtiendra la table en répétant six fois la première table ; on construira ainsi une suite ordonnée de groupes de deux nombres divisée en autant de parties que de fois où on répète la première table. Dans la première partie, les nombres de la première table sont précédés par l'unité ; dans la seconde, ils sont précédés par 2, dans la troisième par 3, dans la quatrième par 4, dans la cinquième par 5, dans la dernière par 6. Il y aura donc en tout 36 petites lignes dans cette table.

La troisième table, relative au cas de trois anneaux, procède de la seconde répétée six fois, et se divise également en 6 parties. Sa première partie, ou premier ordre, sera obtenue en préposant l'unité

---

1. Nous reprenons ici le mot latin « revolutio » qui vient du vocabulaire astronomique.
2. Quand les quatre osselets jetés en l'air présentaient, après être retombés, quatre figures différentes, on avait le coup dit de Vénus.
3. Cicéron, *De Divinatione*, liber I, 13. Cf. *De la Divination. Du Destin. Académiques*, traduction nouvelle de Charles Appuhn, Librairie Garnier, p. 25.

devant chacune des petites lignes de la seconde table ; en préposant de la même façon les nombres 2, 3, 4, 5, 6, on obtiendra les autres parties qui toutes comporteront ainsi le même nombre de termes. En tout, cette troisième table comportera 216 termes.

Nous en arrivons enfin au terme de notre recherche, à la quatrième table relative au cas de quatre anneaux. Elle sera formée, selon la même procédure que précédemment, en répétant six fois la troisième table. Sa première partie, ou premier ordre, sera formée en plaçant l'unité devant les 216 petites lignes de la troisième table ; on continuera de procéder ainsi pour les autres parties, avec les nombres 2, 3, 4, 5, 6. L'étendue de la quatrième table sera donc de 1 216 petites lignes.

J'ai disposé ci-dessous les tables selon l'ordre qu'on vient de fixer. La dernière d'entre elles, répondant à la question posée, montrera, sans qu'aucune soit omise, toutes les révolutions de quatre anneaux, distinctes entre elles. La méthode de construction de ces tables ressort en toute clarté de ce qui précède.

Table 1

1
2
3
4
5
6

Table 2

11
12
13
14
15
16
21
22
23
24
25
26
31
32
.
.
.

Table 3

111	211	311	. . .	611
112	212	312		612
113	.	.		.
114	.	.		.
115	.	.		.
116	.	.		.
121	.	.		.
122	.	.		.
123	.	.		.
.	.	.		.
.	.	.		.
.	.	.		.
.	.	.		.
.	.	.		.
.	.	.		.

Partant de la première table, on peut considérer un nombre de tables aussi grand qu'on voudra ; pour calculer combien chacune d'elles comporte de petites lignes, on use de la multiplication par six sous la forme suivante. En multipliant 6, nombre des premiers caractères, par lui-même, on obtient 36 petites lignes pour la seconde table. En multipliant à nouveau par 6 ce dernier nombre, cela donnera 216 pour la troisième table. De 216 multiplié derechef par 6, il résulte 1 296 petites lignes pour la table qui fait ici l'objet de notre enquête.

Or s'il paraît à propos de considérer la cinquième table, relative à cinq anneaux, on en constituera la première partie ainsi que les suivantes, selon l'enseignement qui ressort des cas précédents jusqu'à ce qu'on arrive à 7 776 petites lignes. Ce qui est le produit de 1 296 multiplié par 6. De même, en multipliant ensuite 7 776 par 6, viendra, pour la sixième table, le nombre de 46 656 petites lignes.

Par ailleurs, puisque, comme il a été dit, ce sont des lettres qui sont gravées sur les anneaux, voyons comment on peut faire correspondre ces lettres aux nombres portés dans la quatrième table.

Supposez que soient tracées les six lettres OFCSDA sur le premier anneau, les lettres VIOAEM sur le deuxième, les lettres IDLNVA sur le troisième, les lettres REIAST sur le quatrième. Prenez maintenant chacun de ces groupes de six lettres, et imaginez que chacune des lettres qui y sont comprises corresponde à un chiffre déterminé choisi parmi : 1, 2, 3, 4, 5, 6, selon l'ordre que vous jugerez bon, comme je l'ai fait par exemple dans le tableau suivant.

1	3	2	6	5	4
O	F	C	S	D	A
3	4	5	2	1	6
V	I	O	A	E	M
6	1	2	4	5	3
I	D	L	N	V	A
4	1	5	3	6	2
R	E	I	A	S	T

En lisant dans l'ordre, de haut en bas, ce tableau, une des six lettres de chacune de ses lignes étant prise chaque fois, on verra les mots OVIR, FIDE, COLI, SANA, DEUS, AMAT. En notant les chiffres qui sont placés dans le tableau au-dessus de chacune des lettres de ces mots, on verra que correspondent respectivement à ces mots, les nombres 1364, 3411, 2525, 6243, 5156, 4632. Ce sont là autant de petites lignes dispersées dans la table relative au cas de quatre anneaux.

On formera aussi d'autres mots en choisissant autrement une lettre dans chacun des anneaux ; ainsi : FIAT, SILE, DIVI, AVLA, auxquels se rapportent les nombres 3432, 6421, 5455, 4323.

Celui qui, ignorant le mot-clef, veut ouvrir la serrure, fera méthodiquement des essais, en tournant chacun des anneaux, selon l'ordre de la quatrième table qu'il suivra à partir de sa première ligne ; il tentera chaque fois de tirer la tige centrale jusqu'à ce qu'elle soit effectivement dégagée et laisse s'ouvrir la serrure. Cela arrivera ; aucun doute n'est permis là-dessus : impossible en effet de réussir en dehors des cas compris dans la table.

Et c'est ainsi que le calculateur, en ouvrant la serrure, perce le secret de l'artisan et surpasse ce dernier par son intelligence. C'est ce qu'on s'était proposé de montrer.

● LE CALCULATEUR OUVRE LA SERRURE

D'auteur qui, au XVI^e^ ou au XVII^e^, ait repris ce problème à nouveaux frais, il n'en est pas à notre connaissance, en dehors de Borrel. C'est de ce dernier que, directement ou indirectement, se font l'écho quelques textes qui méritent pourtant qu'on en dise un mot : la présentation qu'ils en donnent, les autres problèmes auxquels ils la rattachent, placent la « Question » de Borrel sous un nouvel éclairage.

A la fin d'un ouvrage de cryptographie digne d'attention [1], G. Selenus (pseudonyme d'Auguste II, duc de Brunswick et Lunebourg), a reproduit le texte de Borrel ; ce qu'il justifie au nom d'une classification générale dont il ne pousse guère loin les conséquences, mais qui est assez curieuse par elle-même. Un procédé cryptographique consiste à cacher des notions au moyen d'une écriture appropriée ; la théorie du décryptement enseignera comment on peut retrouver ces Notions masquées par les « chiffres ». Or ce qui peut se cacher se partage en Notions, Faits, Effets Artificiels.

Et de même que lorsqu'on décrypte un message, on procède à une « Detectio » des Notions, il y aura également une « Detectio » des Faits cachés [2] ainsi qu'une « Detectio » des Effets Artificiels [3]. C'est évidemment sous cette rubrique que se place l'ouverture des serrures selon la méthode enseignée par Borrel. Selenus compte que son lecteur trouvera quelque agrément à cet exercice qui, ajoute-t-il, a aussi « beaucoup de choses en commun avec ce dont nous avons traité précédemment » : la cryptographie conduit en effet naturellement à des problèmes et à des dénombrements tout à fait analogues.

Deux mots à retenir dans un recueil de récréations mathématiques et physiques [4] du père jésuite C. Schott. Il qualifie de *mathématiques* ces serrures : « Il nous paraît à propos de les appeler *mathématiques* puisqu'elles ne peuvent être construites, fermées, ouvertes, sinon par un artifice mathématique ». Cette

1. *Cryptomenytices et cryptographiae libri IX*, Lunebourg, 1624.
2. « De detectione Facti Occulti Logistica » (*op. cit.*, p. 485-488).
3. « De Serae Buteonicae Reseratione Logistica » (*op. cit.*, p. 489-493).
4. *Ioco-seriorum naturae & artis, sive magiae naturalis centuriae tres*, s.l.n.d., Propositio LI : « Clavem serae mathematicae reperire, & seram aperire », p. 238-239.

caractérisation resterait assez vague, si un second mot bien plus significatif à nos yeux, ne venait la spécifier : le mot de « combinaisons » : « Pour retrouver la formule d'ouverture, lorsqu'on l'a perdue ou qu'on l'ignore, il faut former toutes les combinaisons de toutes les lettres » (« faciendae sunt omnes omnium litterarum combinationes »). Et c'est en termes de « combinaisons » que Schott expose les calculs qu'avait effectués Borrel [1]. Circonstance qui prend toute sa signification du fait que dans les propositions précédentes, Schott avait traité de problèmes de permutations et d'arrangements appliqués en particulier au domaine des anagrammes [2].

Et c'est ainsi que ces « serrures mathématiques » en arrivent à prendre la place qui leur revient dans l'art dont elles ne sont qu'une application parmi d'autres : l'*art combinatoire*. On ne s'étonnera donc pas de les retrouver dans l'encyclopédie des usages de cet art qu'est le *De Arte Combinatoria* de Leibniz [3]. Ce dernier rapproche leur principe de celui qui régit l'utilisation des « roues mobiles » dont les disciples de Lulle faisaient grand usage : ces disques concentriques où sont portées des lettres, et qu'on déplaçait les uns par rapport aux autres pour obtenir tous les groupements possibles entre ces lettres. Sans rien exagérer, on pourrait dire que le problème des cadenas à secret connaît une « postérité multiple dans l'œuvre de Leibniz », à commencer par le thème de la machine à calculer [4] ; amplifié par une multiplicité d'idées harmoniques, le dénombrement appliqué de Borrel peut être érigé en véritable modèle épistémologique [5].

*
* *

Mélancolique épilogue : au ton triomphant du mathématicien du XVI^e^ siècle répond, au XVIII^e^, dans l'*Encyclopédie*, une note désabusée. Rien ne sert de savoir combiner ; encore faut-il qu'on vous laisse le temps d'exercer votre art :

« Mais, dira-t-on, comment ouvre-t-on ce *cadenat* ? C'est par le moyen de signes & de caracteres répandus en grand nombre sur toutes les circonférences des plaques enfilées. Il n'y a qu'une seule position de tous ces caracteres, qui donne aux plaques celle dans laquelle on peut faire sortir la broche du canon ; & il n'y a que le maître du cadenat qui connoisse cette position, & qu'un Géometre qui epuiseroit les combinaisons de tous les caracteres, & qui eprouveroit ces combinaisons de caracteres les unes après les autres, qui puisse rencontrer la bonne ; mais par malheur, cette espece de *cadenat* est à l'usage de gens, dont l'humeur inquiete ne laisse guere aux autres le tems de faire un si grand nombre d'epreuves. » [6]

---

1. Schott ne fait pas mention ici de Borrel, mais c'est de lui que, très vraisemblablement, il a tiré l'idée de ce développement. Il cite en effet Borrel, à une autre occasion, dans le même ouvrage.
2. *Op. cit.*, p. 232-237.
3. Cf. *Die philosophischen Schriften von G. W. Leibniz*, ed. Gerhardt, tome 4, p. 74-75. Leibniz donne les références suivantes : « Vide de his Seris armillaribus Weckerum in Secretis, Illustrissimum Gustavum Selenum in Cryptographia, fol. 449, Schwenterum. in Deliciis Sect. 15. prop. 25. » Nous avons cité plus haut les ouvrages de Weckerus et de Selenus. Daniel Schwenter dans ses *Deliciae physico-mathematicae*..., Nuremberg, 1636, p. 548-550, se contente de suivre le texte de Selenus.
4. Cf. l'étincelant ouvrage consacré récemment à Leibniz par Michel Serres *(Le système de Leibniz et ses modèles mathématiques*, Paris, P.U.F., 1968, tome II, p. 635, n° 1).
5. *Id.*, p. 402-403, p. 428-429, p. 496 sqq.
6. *Encyclopédie ou Dictionnaire raisonné des sciences, des arts et des métiers*, tome second, Paris, 1751, p. 512.