Les machines algorithmiques universelles de Gurevich

Patrick Cegielski
cegielski@univ-paris12.fr

Février 2008

Pour Irène et Marie

Legal Notice

Université Paris XII - IUT
Route forestière Hurtault
F-77300 Fontainebleau
cegielski@univ-paris12.fr

Table des matières

Table des figures

Chapitre 1

La formation de la notion d'algorithme

La notion d'*algorithme* est universellement utilisée, surtout depuis l'apparition des ordinateurs. Cependant, si la notion de fonction algorithmiquement calculable a été étudiée avant l'apparition des ordinateurs, celle d'algorithme elle-même n'a reçue de définition formelle que ces toutes dernières années. L'objet de ce livre est d'en donner une définition formelle (la seule qui existe actuellement, due à Yuri Gurevich). Nous allons rappeler le contexte de celle-ci dans ce premier chapitre en dégageant les quatre moments clès de l'histoire de cette notion :

- le contexte, c'est-à-dire les besoins en calculs de plus en plus complexes, depuis la Préhistoire ;
- la présentation informelle des algorithmes, c'est-à-dire de la façon de réaliser des calculs complexes, depuis la plus haute Antiquité ;
- la définition de ce qui peut être résolu algorithmiquement au milieu des années 1930, cristallisée par la thèse de Church-Turing ;
- et enfin la définition formelle de ce qu'est un algorithme lui-même, cristallisée par le modèle des ASM de Yuri Gurevich et la thèse du même auteur selon laquelle on est bien arrivé à une définition satisfaisante.

Remarquons qu'un autre moment clé :

- la réalisation de machines pour mettre en œuvre les algorithmes ;

est important (il serait impossible de mettre en œuvre certains algorithmes sans elles) mais qu'il peut presque être ignoré pour le but théorique que nous nous sommes assignés.

1.1 Les besoins en calculs

1.1.1 La naissance du calcul arithmétique

Le dénombrement.- Les entiers naturels ont été introduits dès la Préhistoire pour *compter*, c'est-à-dire *dénombrer* les ensembles [finis] concrets (de moutons et autres).

La première façon de dénombrer consiste à *apparier*, c'est-à-dire à mettre en bijection deux ensembles concrets. Il nous reste très peu de témoignage à cet égard mais Karl Absolom ([Abs37]) a trouvé en 1937, en Moravie (République Tchèque), un os appartenant à un jeune loup (voir figure 1-1) qui montre une suite de cinquante cinq incisions disposées en deux séries, par groupes de cinq. Cet os fut découvert dans des sédiments datant de 30 000 ans environ.

FIG. 1.1 – Appariement sur os de loup ([BJBd76],p. 2)

Apparition du calcul arithmétique.- Lors de la naissance des cités, à la fin du Néolithique, le dénombrement prend une importance considérable, à la fois pour comptabiliser les réserves (communes) et pour déterminer les impôts (servant à déterminer la part de chacun dans l'effort commun). C'est certainement à cette époque qu'apparaissent les quatre opérations arithmétiques (addition, multiplication, soustraction, division) et donc le *calcul*, pour la réalisation de ces tâches, bien que nous n'ayons aucun témoignage à cet égard.

Prenons l'exemple de l'addition (des entiers naturels). À cette époque, on ne peut plus se satisfaire de dénombrer les têtes de bétail en les comptant une à une : l'ensemble à dénombrer est trop imposant, d'une part ; on ne peut pas les laisser en place le temps de les compter, d'autre part. Une nouvelle méthode astucieuse apparaît : un fonctionnaire compte celles d'un parc, un autre d'un autre parc et ainsi de suite ; on en fait la somme pour déterminer le nombre de têtes du quartier, puis celui de la cité.

Le fonctionnaire, pour compter les têtes de bétail d'un parc, se contente de mettre un caillou dans une boîte au passage de chaque bête. La boîte est envoyée au quartier, le contenu en est versé dans une boîte plus grande, puis au cœur de la cité. Là on verse le contenu de toutes les boîtes et on compte le nombre de cailloux, ce qui correspond au nombre recherché.

Cette méthode, dite *du berger*, était encore utilisée à la fin du XIX^e siècle, époque à laquelle les historiens des mathématiques la relevèrent. L'utilisation de cette méthode à la fin du Néolithique fut brillament confirmée par Denise Schmandt-Besserat en 1979 [1]. La méthode du berger est encore utilisée couramment dans la Rome Antique, d'où l'étymologie du mot *calcul* (cailloux se disant *calculus* en latin).

Numération unaire.- On a vu avec l'os de jeune loup une façon de représenter un nombre : une incision par élément. Cette *représentation unaire* est une avancée considérable par rapport à la méthode du berger. Elle permet de ne pas avoir à déplacer une grande quantité de matière : seulement un os au lieu de tout un troupeau ou d'une boîte de cailloux.

Le principe du groupement.- Si la représentation unaire correspond à une avancée considérable par rapport au transport d'une boîte de cailloux, elle n'est cependant pas très lisible pour des nombres assez grands. La *méthode du groupement* facilite la lecture. On ne connaît pas l'origine de cette façon de faire mais elle est très ancienne puisque nous avons vu le groupement par cinq sur l'os de loup. Tout ce que l'on peut dire c'est que, dans l'Histoire, ces groupements se sont fait par deux, cinq, dix, vingt et soixante, quelquefois avec un mélange de ces différentes *bases*.

Apparition des systèmes de numération additifs.- Les **systèmes de numération additifs** possèdent des symboles distincts pour chaque sorte de groupe rencontré durant le processus de dénombrement et ce symbole est répété aussi souvent que nécessaire pour indiquer combien on a besoin de chaque groupe.

Le premier exemple historique qui nous soit parvenu est le système de numération égyptien. Intéressons-nous cependant à un autre système, dont une variante est encore utilisée de nos jours : l'ancien système romain (c'est-à-dire avant les formes soustractives IV pour 4 et IX pour 9, ces dernières formes n'apparaissant qu'au Moyen Âge). Il est possible de représenter tout nombre entier inférieur à 5 000 par une suite de symboles (M = 1 000, D = 500, C = 100, X = 10, V = 5 et I = 1) dans laquelle un même symbole apparaît au plus quatre fois : par exemple 2 976 s'écrit MMDCCCCLXXVI. Bien qu'il soit habituel d'écrire les symboles dans l'ordre décroissant des valeurs, ceci n'est pas nécessaire : la valeur d'un symbole dans un système additif n'a rien à voir avec sa position.

Système de numération additif et calculs.- Les systèmes de numération reposant sur le principe de regroupement, non seulement permettent de décrire les nombres de façon concise, mais facilitent également les calculs concernant tout ou partie des quatre opérations arithmétiques.

Les systèmes de numération additifs sont bien adaptés à l'addition et à la multiplication.

[1] Denise Schmandt-Besserat ([SB79, SB92]) montre même que la méthode du berger est à l'origine de l'écriture : au début des tout petits cailloux sont conservés dans des boules en terre cuite à titre de comptabilité ; ensuite le nombre de cailloux est marqué de façon symbolique sur les boules ; plus tard, les cailloux eux-mêmes n'ayant plus une grande importance (plus exactement étant redondants), on ne les place plus dans les boules qui sont seulement marquées de la suite de symboles ; enfin, les boules elles-mêmes ne sont plus conservées, les nombres étant reportés sur des tablettes d'argile. Des commentaires seront ajoutés ensuite (bœuf ou mouton). D'étape en étape, on en arrive à l'écriture.

Une addition se fait en deux étapes : on écrit les deux nombres l'un en-dessous de l'autre, en positionnant les symboles d'un même groupe du second en-dessous des symboles de ceux du premier ; on additionne puis on met sous forme canonique en utilisant les regroupements. Effectuons, par exemple, la somme de 2 319 et de 821 (comme dans [Wil85], p. 7) :

```
  2 319 = MM   CCC    X   V IIII
+   821 =    D    CCC  XX       I
--------------------------------
        = MM D CCCCCC XXX V IIIII
        = MM D DC     XXX V V
        = MM DD C XXXX
        = MMM C XXXX              (= 3 140)
```

Effectuer une multiplication est lent mais le principe n'est pas difficile puisqu'on n'a besoin que de mémoriser les multiples de cinq et de dix :

```
  28 = XXVIII
x 12 =    XII

       XXVIII fois I =      XX      V  III
       XXVIII fois I =      XX      V  III
       XXVIII fois X = CC L   XXX
       ------------------------------------
                     = CC L XXXXXXX VV IIIIII
                     = CC L L    XX VV VI
                     = CCC XXX V I            (= 336)
```

Ces systèmes de numération sont moins bien adaptés à la soustraction et à division.

La division, par exemple, s'effectuait en utilisant les deux opérations auxiliaires de *médiation* (division par deux) et de *duplication* (multiplication par deux) grâce à un algorithme décrit en général de nos jours dans les cours d'initiation à la programmation.

Apparition du système de numération de position.- Les **systèmes de numération positionnels** possèdent des symboles pour les petits nombres, appelés **chiffres**. Les groupes de dénombrement, quant à eux, sont entièrement dénotés par la position du chiffre dans la chaîne de caractères dénotant le nombre. On utilise un chiffre nouveau, le chiffre zéro, pour dénoter un groupe vide.

Les systèmes de numération de position sont un peu bien moins adaptés à l'addition et à la multiplication[2] (les utilisateurs doivent apprendre par cœur les tables d'addition et de multiplication). Leur point fort est qu'ils sont, par contre, également adaptés à la soustraction et à la division. Il est évidemment inutile de décrire ici la méthode utilisée pour effectuer ces opérations puisque c'est le système que nous apprenons à l'école de nos jours.

On ne connaît toujours pas exactement l'histoire du système de numération de position. Les Babyloniens utilisaient un embryon de système de numération de position de base soixante. Malheureusement ils ne disposaient du signe zéro que pour une position : il n'était pas possible, avec leur système, de mettre deux ou plusieurs zéros de suite, ce qui rendait les nombres ambigus.

[2] L'algorithme de la multiplication est considéré comme si difficile que l'École Navale le met encore explicitement au programme de son concours d'entrée au début du XIX^{e} siècle.

La première référence que nous connaissons à propos des chiffres dits arabe (mais en fait dus aux Indiens) est un passage de l'évêque syrien Severus Sebokht de 650 (cité dans [Smi25], vol. 2, p. 64) :

> *Je ne parlerai pas de la science des Hindous, un peuple qui n'est pas le même que les Syriens, ni de leurs découvertes subtiles en astronomie, découvertes qui sont plus ingénieuses que celles des Grecs et des Babyloniens, ni de leurs méthodes de calcul de grande valeur et de leurs calculs qui dépassent la description. Je désire seulement dire que leurs calculs sont faits au moyen de neuf signes.*

On remarquera que le zéro n'est pas cité. La première occurrence du zéro que nous connaissions sans ambiguïté apparaît sur une inscription datant de 876 à Gwalior, sur laquelle on voit '50' et '270' ([Dat]).

Le premier siècle de l'empire musulman fut, dans une large part, consacré aux travaux scientifiques. Al-Mamum crée une maison de la sagesse à Bagdad, comparable à l'ancien Musée d'Alexandrie. C'est dans ce contexte que Mohammed ibn-Musa al-Khwarizmi reconnaît la valeur du système indien en 825 et écrit un petit livre expliquant son utilisation [AK92]. Ce livre fut traduit/adapté en latin au XII^{e} siècle, entre autres sous le titre *Liber Algorismi de numero Indorum* (le livre d'al-Khowarizmi sur les nombres indiens), ce qui conduira à utiliser le mot 'algorithme' à propos de la nouvelle méthode pour écrire les nombres entiers et pour effectuer les calculs.

FIG. 1.2 – Algoriste et abaciste

Le premier occidental à enseigner la nouvelle numération, vers 980, est Gerbert d'Aurillac (938-1003), devenu pape en 999 sous le nom de Sylvestre II. Il était allé étudier en Espagne et a certainement appris ce système à Barcelone, alors en contact étroit avec la civilisation arabe. Cependant il ne semble pas comprendre l'importance du zéro [Ger99].

La méthode se développe surtout après la parution du livre de Fibonacci intitulé *Liber abaci*, paru en 1202 [Fib02]. On remarquera que la méthode des abaques est tellement prédominantes qu'elle désigne l'arithmétique, d'où le titre 'Le livre des abaques' alors qu'il n'est jamais fait référence à ceux-ci dans ce livre au sens où nous l'entendons de nos jours.

Abacistes et algoristes.- Il semblerait qu'une rivalité s'ensuive entre les *abacistes* (prétendant que l'utilisation d'un des premiers outils d'aide aux calculs, les abaques, est plus rapide que la nouvelle méthode) et les *algoristes* au Moyen-Âge, ces derniers l'emportant à partir du XV^e siècle. La célèbre figure 1.2, tirée du *Margarita Philosophica* de Gregor Reisch, paru à Freiburg en 1503, montre la coexistence des deux procédés.

1.1.2 Émergence du calcul sur les décimaux

1.1.2.1 Intérêt des décimaux

Les calculs que nous avons vus jusqu'ici ne concernent que les entiers naturels, liés au dénombrement. La notion de mesure, en particulier la mesure des longueurs (que ce soit la mesure des terrains ou d'un morceau d'étoffe), et l'adoption d'une unité de mesure, conduit à diviser cette unité de mesure pour obtenir une mesure plus fine et donc à l'utilisation des fractions ou, le plus souvent, aux nombres décimaux.

Fraction, nombre décimal et nombre réel.- Les réflexions sur les ensembles de nombres à la fin du XIX^e siècle (et leur enseignement en France dans les années 1960 sous le nom de mathématiques modernes) conduisent à bien distinguer l'ensemble des **nombres décimaux** :

$$\mathbb{D} = \{\frac{n}{10^k} \ / n \in \mathbb{Z} \text{ et } k \in \mathbb{N}\}$$

de l'ensemble $\mathbb{Q}$ des rationnels (ou des fractions), d'une part, et de l'ensemble $\mathbb{R}$ des nombres réels, d'autre part. Certains préfèrent parler de **nombre à virgule** pour avoir un concept indépendant de la base.

1.1.2.2 Apparition des nombres sexagésimaux à Babylone

La première apparition des nombres non entiers qui nous soit conservée concerne les **nombres sexagésimaux**, c'est-à-dire l'analogue des nombres décimaux avec une base de soixante au lieu de notre base usuelle de dix.

Boyer ([BM89], p. 33) nous rapporte qu'une vieille tablette babylonienne (numéro 7 289 de la collection Yale) inclut le calcul de la racine carrée à deux ou trois chiffres sexagésimaux après la virgule, la réponse étant en notation modernisée 1 ;24 ;51,10 où une virgule est utilisée pour séparer les parties entière et fractionnaire et un point virgule comme séparateur des positions sexagésimales. L'addition et la multiplication de ces nombres sexagésimaux n'était pas plus difficile que les opérations analogues sur les nombres entiers. Remarquons au passage que, encore en 1968 (et même dans l'édition de 1989), Boyer parle de *fraction sexagésimale* et non de nombre sexagésimal.

1.1.2.3 Table des cordes de Ptolémée

Claude Ptolémée[3] vivait à Alexandrie au II^e siècle après Jésus-Christ à une époque relativement calme qui favorisait les voyages et les explorations. Il décida de

[3]Pour une introduction à l'œuvre de Ptolémée, on pourra consulter [Auj93].

faire la synthèse des connaissances géographiques de son temps dans une œuvre qui alla bien au-delà d'une simple synthèse. Il décrit la terre et le monde habité dans trois ouvrages : la *Syntaxe mathématique* d'abord (plus connue sous le nom d'*Almageste*, le très grand, que lui donnèrent les Arabes), où les diverses composantes du système terre-ciel sont étudiées par la géométrie ; l'*Apotélesmatique*, ou *Tétrabible*, ensuite qui présente un tableau des influences astrales (on dirait plutôt climatiques de nos jours) sur les divers pays et sur leurs habitants ; le *Guide Géographique* enfin (ou, pour faire court, la *Géographie*), qui donne toutes les directives utiles pour tracer une carte générale, et des cartes régionales, du monde habité, avec ses extensions récentes.

La *Syntaxe mathématique* [Pto13, Too98] est une synthèse ordonnée et une mise à jour des connaissances, acquises par la géométrie et l'arithmétique, sur le système du monde et ses différentes composantes. Il commence par rappeler les hypothèses philosophiques (la terre immobile au centre du monde réduite à un point, le ciel comme sphère en mouvement) puis, et c'est là son génie, il va montrer comment, d'une seule donnée concernant la latitude (longueur du jour le plus long, hauteur du pôle, rapport de l'ombre au gnomon), on peut déduire les autres. Il use pour ce faire non seulement de démonstrations géométriques, mais aussi de calculs qui lui sont facilités par les tables trigonométriques qu'il dresse dans le livre I.

Ptolémée crée donc la trigonométrie. La *corde* d'un angle α dans un cercle de rayon R (voir figure 1.3) est la longueur $cord(\alpha)$ de la corde correspondant à un arc

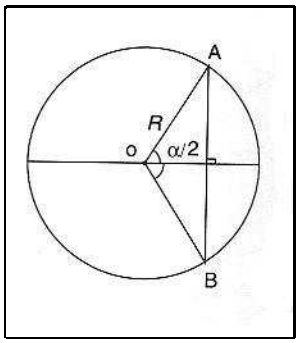


FIG. 1.3 – Corde

de cercle sous-tendu par un angle au centre α.

La notion de corde a été remplacée par celle de sinus au VI^e siècle en Inde par Aryabhata. Il est facile de voir que le rapport d'une corde au diamètre est égal au sinus de l'angle moitié : $cord(\alpha) = 2Rsin(\alpha/2)$.

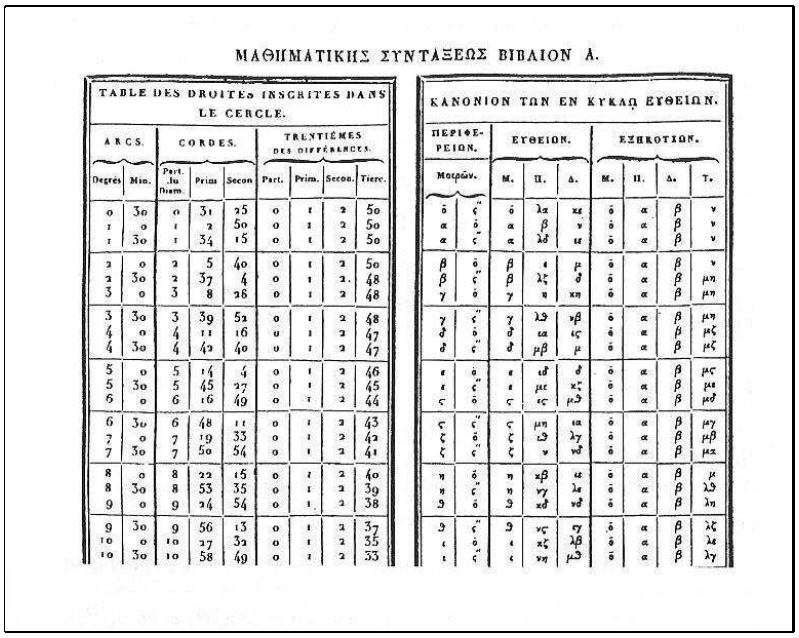
Ptolémée établit une table des cordes de demi-degré en demi-degré, avec une approximation correspondant à presque six décimales exactes. Il utilise la division babylonienne du cercle en 360^o et calcule en numération sexagésimale. Il suppose que le diamètre est partagé en 120 parties égales, si bien que l'unité de longueur de corde sera la partie (^{p}), divisée à son tour en minutes (') et en secondes (").

Ptolémée explique comment il détermine sa table :

– 1) *Détermination de* $cord(72^o)$ *et* $cord(36^o)$. Il commence par construire géométriquement les côtés du pentagone et du décagone réguliers, qui sous-tendent respectivement des arcs de 72^o et de 36^o. Il en déduit, par utilisation itérée du théorème de Pythagore, les valeurs :

$$cord(72^o) = 70^p32'3'' \text{ et } cord(36^o) = 37^p4'55''.$$

- 2) *Théorème de Ptolémée.* Il démontre ensuite le résultat, actuellement connu sous le nom de *théorème de Ptolémée* : dans un quadrilatère inscrit ABCD, le produit des diagonales est égal à la somme des produits des côtés opposés.
- 3) *Corde de la différence de deux angles.* Avec l'énoncé précédent, il montre comment, quand on connaît les cordes de deux angles α et β, on peut calculer la corde de la différence $\alpha-\beta$. Il s'agit de l'analogue du théorème sur $sin(\alpha-\beta)$. À partir de la corde de 72^o déjà calculée et de celle de 60^o, facile à déterminer, on en déduit la valeur de la corde de 12^o.
- 4) *Corde d'un arc moitié.* Ptolémée explique ensuite comment, quand on connaît la corde d'un angle, on peut calculer la corde de l'arc moitié. On en déduit les valeurs des cordes des angles 6^o, 3^o, $3/2^o$ et $3/4^o$.
- 5) *Corde de 1°.* Le procédé précédent ne permettant d'obtenir ni $cord(1^o)$, ni *a fortiori* $cord(1/2^o)$, Ptolémée utilise un encadrement subtil qui lui fournit la valeur de $cord(1^o)$, puis de $cord(1/2^o)$ avec une précision suffisante pour son projet.
- 6) *Table de demi-degré en demi-degré.* Ptolémée établit alors sa table selon la technique précédente en tenant compte aussi de ce que, grâce au théorème de Ptolémée, quand on connaît les cordes de deux angles α et β, on peut calculer la corde de la somme $\alpha+\beta$.



ΜΑΘΗΜΑΤΙΚΗΣ ΣΥΝΤΑΞΕΩΣ ΒΙΒΛΙΟΝ Α.

TABLE DES DROITES INSCRITES DANS LE CERCLE.

ARCS.		CORDES.			TRENTIÈMES DES DIFFÉRENCES.			
Degrés	Min.	Part. du Diam.	Prim.	Secon.	Part.	Prim.	Secon.	Tierc.
0	30	0	31	25	0	1	2	50
1	0	1	2	50	0	1	2	50
1	30	1	34	15	0	1	2	50
2	0	2	5	40	0	1	2	50
2	30	2	37	4	0	1	2	48
3	0	3	8	26	0	1	2	48
3	30	3	39	52	0	1	2	48
4	0	4	11	16	0	1	2	47
4	30	4	42	40	0	1	2	47
5	0	5	14	4	0	1	2	46
5	30	5	45	27	0	1	2	45
6	0	6	16	49	0	1	2	44
6	30	6	48	11	0	1	2	43
7	0	7	19	33	0	1	2	42
7	30	7	50	54	0	1	2	41
8	0	8	22	15	0	1	2	40
8	30	8	53	35	0	1	2	39
9	0	9	24	54	0	1	2	38
9	30	9	56	13	0	1	2	37
10	0	10	27	32	0	1	2	35
10	30	10	58	49	0	1	2	33

KANONION ΤΩΝ ΕΝ ΚΥΚΛΩ ΕΥΘΕΙΩΝ.

ΠΕΡΙΦΕΡΕΙΩΝ.		ΕΥΘΕΙΩΝ.			ΕΞΗΚΟΣΤΩΝ.			
Μοιρῶν.		Μ.	Π.	Δ.	Μ.	Π.	Δ.	Τ.
ὁ	ς′	ὁ	λα	κε	ὁ	α	β	ν
α	ὁ	α	β	ν	ὁ	α	β	ν
α	ς′	α	λδ	με	ὁ	α	β	ν
β	ὁ	β	ε	μ	ὁ	α	β	ν
β	ς′	β	λζ	θ	ὁ	α	β	μη
γ	ὁ	γ	η	κη	ὁ	α	β	μη
γ	ς′	γ	λθ	νβ	ὁ	α	β	μη
δ	ὁ	δ	εα	ις	ὁ	α	β	μζ
δ	ς′	δ	μβ	μ	ὁ	α	β	μζ
ε	ὁ	ε	ιδ	θ	ὁ	α	β	μς
ε	ς′	ε	με	κς	ὁ	α	β	μθ
ς	ὁ	ς	ις	μθ	ὁ	α	β	μθ
ς	ς′	ς	μη	ια	ὁ	α	β	μγ
ζ	ὁ	ζ	κθ	λγ	ὁ	α	β	μβ
ζ	ς′	ζ	ν	νδ	ὁ	α	β	μα
η	ὁ	η	κβ	με	ὁ	α	β	μ
η	ς′	η	νγ	λε	ὁ	α	β	λθ
θ	ὁ	θ	κδ	νδ	ὁ	α	β	λη
θ	ς′	θ	νς	ιγ	ὁ	α	β	λζ
ι	ὁ	ι	κς	λβ	ὁ	α	β	λε
ι	ς′	ι	νη	μθ	ὁ	α	β	λγ

FIG. 1.4 – Table des cordes

Remarquons que les cordes (ou les sinus) sont des nombres réels et non des nombres à virgule. La table contient donc des valeurs approchées mais PTOLÉMÉE ne le dit à aucun moment.

1.1.2.4 Nombres à virgule décimaux

Apparition.- L'utilisation des nombres à virgule décimaux (et non plus sexagésimaux) semble datée du chinois Liu HUI au troisième siècle après Jésus-Christ [Nee59], à propos de l'écriture (de valeurs approchées) de racines carrées. Les calculs sur de tels nombres à virgule sont dominés en 1261, puisque Yang HUI multiplie 24,68 par 36,56 pour obtenir 902,3008. L'utilisation passe à l'Occident *via* les In-

diens et les Arabes. Les tables de RHAETICUS (1551) contiennent les six fonctions trigonométriques pour les angles de 10" en 10" : les résultats sont exprimés sous forme de nombres à virgule décimaux à sept chiffres après la virgule.

Utilisation courante des nombres à virgule.- L'utilisation systématique des nombres à virgule décimaux pour la mesure des longueurs, des aires, des volumes et autres a été défendue par le mathématicien belge Simon STEVIN en 1585 [Ste34] dans son livre intitulé *De Thiende* (le dixième en flamand, traduit en français sous le nom *La disme*). Cependant cette proposition ne sera pas retenue avant la Révolution française.

STEVIN écrit $47\boxed{0}$, $5\boxed{1}$, $8\boxed{2}$ le nombre décimal 47,58. Cela lui permet également d'écrire $2\boxed{3}7\boxed{5}$ pour 0,00207. Il justifie, et c'est le premier à le faire, les opérations sur ces nombres à virgule.

Notion de valeur approchée.- STEVIN est également le premier mathématicien à préciser qu'un nombre à virgule est un nombre approché pour un nombre réel :

> *Il arrive quelquefois que le quotient ne peut pas être exprimé par des nombres entiers, comme dans le cas de* $4\boxed{3}$ *divisé par* $3\boxed{2}$*. Il apparaît ici que le quotient sera indéfiniment trois avec un tiers en addition. Dans un tel cas, nous pouvons approcher autant que l'on veut le quotient réel que le problème l'exige et omettre le reste. Il est vrai que* $13\boxed{0}3\boxed{1}3\frac{1}{3}\boxed{2}$*, ou* $13\boxed{0}3\boxed{1}\ 3\boxed{2}3\frac{1}{3}\boxed{3}$ *soit le résultat exact, mais dans* La Disme*, nous proposons de n'utiliser que les nombres entiers et, de plus, nous notons que en affaires on ne prend pas en compte la millième partie d'un grain. Les ommissions telles que celles-ci sont faites par les principaux géomètres et arithméticiens même dans les calculs d'une grande importance. Ptolémée et Jehan de Montroyal, par exemple, n'ont pas maquillé leurs tables avec la plus haute précision qu'ils pouvaient atteindre avec les nombres mélangés car, au vu du propos de ces tables, l'approximation est plus utile que la perfection.*

Notation actuelle.- L'idée de la notation actuelle des nombres à virgule est due à Christopher RUDOLFF. Celui-ci publie en 1530 à Augsburg un livre comprenant une table d'intérêts composés dans laquelle apparaissent les valeurs de $375 \times (1 + 5/100)^n$ pour n variant de 1 à 10. Les résultats sont exprimés sous forme de fractions décimales, une barre verticale '|' jouant le rôle de notre virgule décimale. On a par exemple 413|4375 pour $n = 2$. Cette table est reproduite p. 241 du volume II de [Smi25].

La notation actuelle, avec un point décimal pour les anglo-saxons et une virgule sur le continent, est due à John NAPIER, l'inventeur des logarithmes. Nous avons vu que le problème du repérage sur une sphère a conduit PTOLÉMÉE à introduire les fonctions trigonométriques. Les tables furent utilisées pour la navigation au long cours. La formule donnant $cos(a + b)$ fait intervenir deux multiplications. NAPIER introduisit les logarithmes pour faciliter le calcul des tables, pour remplacer la multiplication par une addition. Il présenta ses logarithmes (de fonctions trigonométriques) dans un livre écrit en latin, son *Descriptio* de 1614. Ce qui nous intéresse ici est que la notation des nombres à virgule, avec un point décimal, apparaît dans la traduction anglaise de ce livre (écrit en latin) en 1616. Henry BRIGGS utilise la virgule décimale dans sa table de 1624.

Les notations restèrent diverses durant un siècle jusqu'à ce que Léonard EULER la rende standard dans son *Introductio in Analysis Infinitorum* [Eul48] de 1748.

1.1.3 Apparition du calcul sur les fractions

Intérêt des fractions.- La notion de fraction apparaît certainement avec les problèmes de mesure. La mesure des grandeurs n'a pas cependant à être très précise en pratique, aussi l'utilisation des nombres à virgule est-elle suffisante. Les problèmes de change, liés au commerce international en Europe médiévale, par contre nécessitent une agilité dans la manipulation des fractions.

Considérons par exemple Adam Riese [Car65], qui vulgarise les nombres arabes en Allemagne à partir de 1518. La table des matières d'un de ses nombreux livres consacrés à l'enseignement de l'arithmétique est : numération, addition, soustraction, duplication, médiation, multiplication, division, progression, règle de trois, échange des monnaies, profit, calcul de l'argent et de l'or, partenariat et réduction (des fractions). Un des problèmes de change de l'édition de 1559 commence ainsi :

> *Sept florins de Padoue en font cinq à Venise, 10 à Venise en font 6 à Nuremberg, 100 à Nuremberg en font 73 à Cologne. Combien font 1000 fl. de Padoue à Cologne. Cela fait 312 et 6/7.*

On voit tout l'intérêt des fractions exactes pour les problèmes de change. Le numérateur peut être n'importe quel entier.

Apparition des fractions unitaires en Égypte.- Nous ne possédons aucun témoignage sur la naissance des fractions. Les inscriptions en hiérogyphes des Égyptiens (voir sections 1-6 et 1-8 de [BJBd76]) ont une notation spéciale pour les fractions de l'unité, c'est-à-dire les fractions avec un numérateur égal à un : la réciproque d'un nombre entier était indiqué en plaçant un signe d'ovale allongée sur le nombre représentant cet entier. En notation hiératique, l'ovale est remplacée par un point. De telles fractions de l'unité sont utilisées dans le papyrus Rhind mais les fractions les plus générales ne semblent pas être connues.

Les fractions en Grèce.- Sous l'influence des Égyptiens, les Grecs ont commencé par n'utiliser les fractions que comme somme de fractions unitaires (voir la fin de la section 3-2 de [BJBd76]). Ils notent ensuite les fractions de deux façons.

Ils écrivent quelquefois les fractions avec le numérateur suivi d'un accent et le dénominateur écrit deux fois, à chaque fois suivi d'un double accent. Par exemple, en se souvenant que les chiffres grecs sont les lettres dans l'ordre alphabétique, $\frac{2}{3}$ est écrit :

$$\beta'\gamma''\gamma''$$

Ils écrivent aussi le dénominateur sous le numérateur, mais sans utiliser notre barre de fraction :

$$\begin{matrix}\beta \\ \gamma\end{matrix}$$

Les fractions et les taux de change.- Comme nous l'avons déjà dit, l'utilisation des fractions prendra tout son sens avec les problèmes de taux de change. Ceci deviendra d'usage courant après la publication du *Liber Abaci* [Fib02] de Fibonacci en 1202 et de *La Disme* de Simon Stevin en 1585 [Ste34].

1.1.4 Les réels comme idéalisation des décimaux

Nous venons de voir les calculs (ou plus exactement les quatre opérations que sont l'addition, la multiplication, la soustraction et la division) sur trois ensembles de nombres (entiers naturels, nombres décimaux et nombres rationnels positifs).

Faisons une petite digression à propos d'un ensemble de nombres, celui des réels, pour lesquels ces quatre opérations sont définies mais à propos duquel on ne parle pas de calcul.

Découverte des irrationnels.- Le fait que tout nombre, introduit de façon naturelle, n'est pas nécessairement un nombre rationnel (une fraction) est une découverte de l'École de PYTHAGORE [vF45] au VI^e siècle avant J.-C. Le théorème de Pythagore conduit à considérer la longueur d'une diagonale de carré l'unité, ce que nous notons $\sqrt{2}$, dont on montra que ce ne pouvait pas être un nombre rationnel. Cette découverte était si contraire à la philosophie de l'École de PYTHAGORE (pour qui tout était nombre, sous-entendu entier ou quotient d'entiers) qu'il fut interdit d'en révéler l'existence à l'extérieur de l'école. Une légende veut qu'un certain HIPPASE de Métaponte ait divulgué la découverte et qu'il fut englouti dans les flots (sous-entendu par vengeance ou par suicide causé par les remords).

On ne connaît pas la démonstration de l'École de PYTHAGORE. La première démonstration connue, celle qui est encore donnée de nos jours, date de deux siècles plus tard (ARISTOTE, *Analytiques Postérieurs*, [Ari47] I 23).

THÉODORE montra au IV^e avant J.-C. que $\sqrt{3}$, $\sqrt{5}$, ..., $\sqrt{17}$ sont aussi des irrationnels. Une méthode générale fut certainement trouvée par THÉÉTHÈTE (413–369) pour montrer que la racine carrée d'un entier qui n'est pas un carré est irrationnelle.

Définition des nombres réels.- EUDOXE de Cnide (408–355) va résoudre la *crise des irrationnels* en donnant la définition d'un nouvel ensemble de nombres, sous une forme qui nous est inconnue puisque toute son œuvre est perdue. La théorie des rapports d'EUDOXE est cependant reprise dans le livre V des *Éléments* [Euc19] d'EUCLIDE (vers 300 avant J.-C.), selon les dires de PROCLUS au V^e siècle après J.-C [Pro48]. Ce livre des *Éléments* est de lecture difficile mais Jean DHOMBRES (voir [Dho78]) en donne une interprétation moderne comme définition d'un demi-corps totalement ordonné archimédien maximal.

Cette définition suffira jusqu'au moment où on se penchera sur les fondements de l'Analyse. Charles MÉRAY, Karl WEIERSTRASS et Georg CANTOR donneront trois constructions de l'ensemble des nombres réels en 1870, qui se révèleront équivalentes. David HILBERT en donnera une définition axiomatique (analogue à l'interprétation de DHOMBRES citée ci-dessus) en 1900.

Théorie et pratique.- La distinction entre nombres décimaux et nombres réels n'est pas claire jusqu'en 1870, ou tout au moins fait-on semblant. On raisonne sur les réels, on calcule avec les décimaux en espérant que les erreurs commises peuvent être considérées comme négligeable. La notion de calcul sur les réels, avec des algorithmes, n'apparaît donc jamais.

En fait ceci est impossible comme le montreront les réflexions sur la calculabilité dont nous parlerons plus tard.

1.1.5 Vers une notion générale de calcul

Calculs sur d'autres entités.- Si on a des opérations sur les réels mais qu'on n'y parle pas de calcul, il n'en est pas de même pour d'autres entités. Ainsi lorsque Isaac NEWTON et LEIBNIZ facilitent le 'calcul' des volumes au XVII^e siècle (avancée considérable par rapport à la méthode d'exhaustion utilisée jusqu'alors, pour laquelle il fallait deviner le résultat avant de pouvoir le justifier) et autres applications par une nouvelle méthode suffisamment générale, on parlera de 'calcul intégral' et de 'calcul différentiel'. Ces noms désignent de nos jours deux sous-disciplines de l'Analyse mais le 'calcul différentiel', par exemple, ne devrait être réservé en toute rigueur

qu'au chapitre de cette discipline qui indique comment déterminer la dérivée d'une fonction en s'aidant de dérivées élémentaires et des théorèmes sur les opérations (arithmétiques, composition et réciproque).

Plusieurs mots pour un même concept.- Le cas de l'arithmétique est simple de nos jours : pour déterminer le cardinal d'un ensemble fini donné, soit on dénombre (en désignant les éléments de l'ensemble un à un), soit on calcule (en utilisant les quatre opérations d'addition, de soustraction, de multiplication et de division), soit on fait appel à des opérations plus compliquées étudiées dans la discipline appelée Analyse combinatoire.

Le vocabulaire a fortement changé au cours des siècles. Dans la Grèce Antique, on distingue la *logistique*, notre arithmétique élémentaire, et l'arithmétique (que nous appelons plutôt théorie des nombres de nos jours). Nous avons vu que le fait de calculer se dit souvent en faisant référence à l'abaque. On parlera d'algorithme au Moyen-Âge en déformant le nom d'un auteur du monde mulsulman.

Un même mot pour plusieurs concepts.- Nous avons vu également la naissance de l'établissement des tables avec Ptolémée, ce qui conduit à des calculs complexes. Aucune réflexion d'ensemble ne semble être effectuée sur cette apparition, de plus en plus considérable, de calculs des plus complexes.

1.2 Présentation informelle des algorithmes

Les algorithmes apparaissent dès les premières civilisations de l'époque historique (c'est-à-dire possédant l'écriture, rappelons-le) connues, Mésopotamie et Égypte. La présentation des algorithmes varie évidemment selon celles-ci.

1.2.1 Les algorithmes en Mésopotamie

L'étude systématique des mathématiques mésopotamiennes date des travaux de Otto Neugebauer ([Neu35] et [NS45]) en Allemagne et de François Thureau-Dangin en France [TD38]. On peut classer les textes mathématiques babyloniens en deux catégories : les tables numériques et les tablettes de problèmes. Les premières ne sont pas différentes des tables modernes : des nombres disposés en colonnes, ordonnés selon des séries croissantes ou décroissantes. Les tablettes de problèmes sont des recueils d'exercices, comme on en trouve à la fin de nos manuels scolaires. Ce sont certainement des recueils didactiques car dans bien des cas ils supposent des précisions que l'énoncé ne fournit pas et qui devaient être indiquées oralement à l'élève.

Considérons par exemple le premier problème étudié par Thureau-Dangin, celui de la tablette 13 901 du British Museum :

> *La surface du carré ajoutée au côté égale ;45. Tu poseras 1, l'unité. Tu fractionneras 1 en 2. On trouve ;30. Tu croiseras ;30. On trouve alors ;15. Tu ajouteras ;15 et ;45. On trouve 1. C'est le carré de 1. Tu soustrairas de 1 les ;30 que tu as croisés. On trouve ;30. C'est le côté du carré.*

Traduit avec des notations algébriques modernes, cela donne :

On veut résoudre l'équation $x^2 + bx = c$, en prenant comme exemple b = 1 et c = ;45.

L'unité, c'est-à-dire le coefficient b de x, est ici égale à 1.

On divise b par deux. On trouve dans notre cas $\frac{b}{2} =; 30$.

On l'élève au carré. On trouve dans notre cas $(\frac{b}{2})^2 =; 15$.

On ajoute $(\frac{b}{2})^2$ et c. On trouve dans notre cas $(\frac{b}{2})^2 + c = 1$.

On détermine la racine carrée. On a dans notre cas $\sqrt{(\frac{b}{2})^2 + c} = 1$.

On soustrait ce qu'on a élevé au carré, c'est-à-dire $\frac{b}{2}$ rappelons-le. On obtient dans notre cas : $\sqrt{(\frac{b}{2})^2 + c} - \frac{b}{2} =; 30$.

C'est le côté du carré voulu. Dans notre cas $x =; 30$.

Exercice.- *Justifier l'algorithme.*

1.2.2 Les algorithmes en Égypte

Les plus anciens textes mathématiques égyptiens connus contiennent principalement des problèmes de nature pratique, tels que des calculs de capacité, le nombre de briques nécessaires pour construire un mur ou le stock de grains nécessaire pour la préparation d'une certaine quantité de pain ou de bière.

La principale source d'information est le *papyrus Rhind* [Cha27] (nom qui lui est donné en hommage à l'anglais A. Henry Rhind qui l'a acheté à Louxor en 1858 et revendu au British Museum). Il existe quatre autres documents, de moindre importance : le *payrus de Moscou*, le *papyrus Kahun*, le *papyrus de Berlin* et le *rouleau de cuir*. L'intégralité de ces cinq documents est traduit dans [Cla99].

Les algorithmes ressemblent à ceux de la Mésopotamie. Considérons par exemple le probème 26 du papyrus Rhind :

> *Une quantité et son quart font 15. Quelle est la quantité ? La solution est la suivante : calculer avec 4 ; prends le quart, 1 ; ensemble 5 ; calculer avec 5 pour obtenir 15, soit 3. On a 4×3. Ainsi 12 est le résultat.*

Le principe de cette méthode sera appelé plus tard la méthode de la fausse position.

1.2.3 Pas d'algorithme en Grèce

Les Grecs faisaient une distinction très nette entre l'*arithmétique* (*arithmetike'*, de *arithmos'*, nombre), qui correspond à notre théorie des nombres, et *logistique* (*logistike'*), qui désigne l'art du calcul, si on en croit *La République* [VII 522-526] de Platon (429–347). L'attitude des Grecs à l'égard des arts et métiers était que ceux-ci n'étaient pas dignes d'attention et réservés aux eslaves. Nous ne possédons donc que peu de témoignages sur la logistique. Nous avons peu de chances de trouver des présentations d'algorithmes comme en Mésopotamie ou en Égypte.

Ces deux branches, arithmétique et logistique, seront traitées séparément jusqu'au début de l'imprimerie.

1.2.4 Les algorithmes en Chine

L'ouvrage mathématique classique se nomme *Les Neuf Chapitres*, dont nous disposons d'une édition française depuis 2004 [CS04], et date de 2 000 ans environ. Il s'agit d'une liste d'algorithmes pour des problèmes divers. Chaque problème donne lieu à plusieurs exemples numériques suivis d'une procédure générale.

Citons par exemple le problème (1.21) (pp. 169–171 de la traduction française) :

> (1.21)
>
> Supposons maintenant qu'on ait un champ de 4/5 de *bu* de largeur, et de 5/9 de *bu* de longueur. On demande combien fait le champ.
>
> Réponse : 4/9 de *bu*[4].

[4] carré.

Procédure de la multiplication des parts :

Les dénominateurs multipliés l'un par l'autre font le diviseur ; les numérateurs multipliés l'un par l'autre font le dividende. On effectue la division du dividende par le diviseur.

1.2.5 Apparition des programmes de calcul

Le calcul comme tâche collective.- L'établissement des tables, de plus en plus nombreuses, ne peut plus être le fait d'un seul homme. Au XVI^{e} siècle l'astronome allemand Rheticus employa une équipe de calculateurs durant une dizaine d'années pour établir une table des sinus à quinze décimales avec un pas de 10" pour les angles. Mais on ne connait rien des détails de la méthode utilisée.

Prony.- Gaspard de Prony (1755-1839) (voir [OR97]) est le premier à expliquer sa méthode, issue de la lecture d'Adam Smith.

Adam Smith (1723-1790), dans le chapitre un du livre un de sa *Richesse des Nations* de 1776 ([Smi76]), insiste sur l'intérêt de la division du travail, illustrant son propos par la manufacture d'épingles :

> *Un homme qui ne serait pas façonné à ce genre d'ouvrage, dont la division du travail a fait un métier particulier, ni accoutumé à se servir des instruments qui y sont en usage, dont l'invention est probablement due encore à la division du travail, cet ouvrier, quelque adroit qu'il fût, pourrait peut-être à peine faire une épingle dans toute sa journée, et certainement il n'en ferait pas une vingtaine. Mais de la manière dont cette industrie est maintenant conduite, non seulement l'ouvrage entier forme un métier particulier, mais même cet ouvrage est divisé en un grand nombre de branches, dont la plupart constituent autant de métiers particuliers. [...] L'important travail de faire une épingle est divisé en dix-huit opérations distinctes ou environ, lesquelles, dans certaines fabriques, sont remplies par autant de mains différentes. [...] J'ai vu une petite manufacture de ce genre qui n'employait que dix ouvriers. [...] Quand ils se mettaient en train, ils venaient à bout de faire entre eux environ onze livres d'épingles par jour ; or, chaque livre contient au delà de quatre mille épingles de taille moyenne. Ainsi, ces dix ouvriers pouvaient faire entre eux plus de quarante-huit milliers d'épingles dans une journée.*
>
> [...]
>
> *Observez, dans un pays civilisé et florissant, ce qu'est le mobilier d'un simple journalier ou du dernier des manœuvres, et vous verrez que le nombre de gens dont l'industrie a concouru pour une part quelconque à lui fournir ce mobilier, est au-delà de tout calcul possible. [...] Il est bien vrai que son mobilier paraîtra extrêmement simple et commun, si on le compare avec le luxe extravagant d'un grand seigneur ; cependant, entre le mobilier d'un prince d'Europe et celui d'un paysan laborieux et rangé, il n'y a peut-être pas autant de différence qu'entre les meubles de ce dernier et ceux de tel roi d'Afrique qui règne sur dix mille sauvages nus.*

Prony, après avoir lu *Richesses des Nations*, a l'idée d'appliquer ce principe de la division du travail au travail mental. Voilà comment Dorothy Stein décrit les travaux de Prony dans sa biographie d'Ada Byron :

> *Le baron Gaspard de Prony était directeur de l'École des Ponts et Chaussées [il ne le deviendra en fait qu'en 1798], lorsqu'il reçut mission en*

> *1792 de la part du gouvernement français de superviser la préparation des nouvelles tables mathématiques qu'exigeait l'adoption du système métrique. Réfléchissant à la façon d'organiser un travail aussi considérable, il tomba par hasard sur un exemplaire de* Richesse des Nations. *Il décida immédiatement de fabriquer ses logarithmes comme des épingles.*
>
> *Il monta deux ateliers qui effectuaient les mêmes calculs et se contrôleraient donc mutuellement. Au-dessus d'eux se trouvaient deux autres sections de travail mental. La première section, composée de cinq ou six mathématiciens parmi les plus éminents de France, était chargée de décider des meilleurs formules à employer pour calculer pas à pas les fonctions qui devaient figurer dans les tables. (Ils exécutaient la tâche des programmeurs.) Ces formules étaient alors transmises à la deuxième section, formée de sept ou huit mathématiciens compétents qui devaient substituer des nombres aux symboles des formules, puis les passer à la troisième section (ceux-ci faisaient fonction de clavistes). La deuxième section devait aussi assurer, au retour des calculs finis, la comparaison et la coordination des résultats.*
>
> *La troisième section comprenait soixante à quatre-vingt personnes qui exécutaient la plus grand partie du travail numérique, en utilisant seulement l'addition et la soustraction.*
>
> [Ste85], pp. 125-126 de la traduction française

Les tables furent achevées en 1801 mais ne seront pas publiées avant la fin du XIX^{e} siècle, car trop onéreuses à imprimer.

1.2.6 Ada Byron et la naissance des programmes

Les tables diverses deviennent indispensables, principalement pour la navigation comme nous l'avons déjà dit. Cependant ces tables comportent des erreurs. Dionysius Lardner, professeur de philosophie naturelle et d'astronomie à l'université de Londres, est un vulgarisateur des sciences prolifique. Dans un article de 1834 [Lar34] il inspecte une collection privée de 140 volumes de tables (certainement celle de Charles Babbage). Dans une sélection aléatoire de 40 volumes, il trouve plus de 3 000 erreurs spécifiées dans les feuilles d'*errata*.

Ces erreurs peuvent prendre naissance lors de n'importe laquelle des trois étapes de la préparation des tables : le calcul, la transcription et l'impression. Charles Babbage (1791–1871) veut éviter ces trois types d'erreur en créant une machine qui fasse les calculs et qui imprime les tables. Il conçoit le premier ordinateur, entièrement mécanique, qu'il n'arrivera pas à réaliser par déficience de l'industrie mécanique de l'époque (un exemplaire sera partiellement réalisé en 1991 pour de bicentenaire de sa naissance).

Babbage essaie d'obtenir des subsides pour construire sa machine. Il en présente le projet à divers endroits, en particulier à Turin :

> *En 1840, Babbage se rendit à Turin pour donner une série de conférences et participer à des discussions dont le but était d'expliquer le projet de la Machine Analytique à un groupe de philosophes et d'hommes de science italiens. Il avait espéré que le plus éminent d'entre eux, le baron Plana, écrirait un article ou un rapport sur le sujet, mais Plana se déroba en invoquant des ennuis de santé. Il dut se contenter, à la fin, du concours d'un jeune ingénieur militaire, le capitaine Luigi Menabrea (qui devait devenir plus tard Premier ministre d'Italie). [...] Il parut, en français, dans la* Bibliothèque Universelle de Genève*, en octobre 1842.*
>
> [Ste85], pp. 117-118 de la traduction française

Les travaux de PRONY sont cités par Luigi MENABREA [Men42], probablement avec l'encouragement de BABBAGE, comme un préalable à la discussion de la *Machine Analytique* de ce dernier.

La notion de programme (d'ordinateur) est due conjointement à Charles BABBAGE et à Lady Ada LOVELACE. Elle apparaît en note dans la traduction anglaise [Men42] que Lady Ada LOVELACE donne de l'article de MENABREA.

1.2.7 Les bureaux de calculs

On a donc employé des hommes moins qualifiés que les mathématiciens pour aider à l'établissement de tables. Il n'est pas nécessaire qu'ils sachent ce qu'est un logarithme, par exemple. On leur communique un plan de calculs à réaliser, avec des cases à remplir. Les anciens instituteurs, en particulier, conviennent bien à cette tâche. Le rôle du mathématicien consiste à établir ce plan de calcul, ce programme ou cet algorithme comme nous dirions de nos jours. Naissent alors les *bureaux de calculs* dans lesquels des employés suivent l'algorithme pour un jeu de données, en effectuant les quatre opérations et en les reportant sur des feuilles sur lesquelles l'emplacement des opérations intermédiaires est marqué. Les employés ne comprennent pas nécessairement le but de cette suite de calculs, mais cela n'a pas d'importance. Les bureaux de calculs deviennent des officines courantes à la fin du XIX^{e} siècle et ne disparaîtront que dans les années 1960 avec l'utilisation courante des ordinateurs.

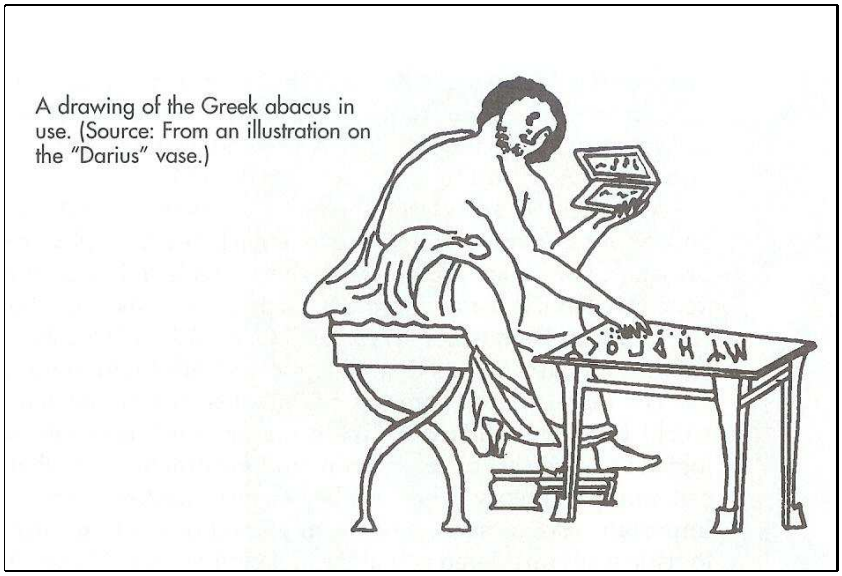


FIG. 1.5 – Vase de Darius ([Wil85], p. 56)

1.3 Machines d'aide aux calculs

1.3.1 Les abaques

L'Antiquité et le haut Moyen Âge n'ont connu que les système de numération additifs. Des outils d'aide aux calculs apparurent très tôt sous le nom d'**abaque**, qui a désigné des techniques différentes et dont l'histoire est en grande partie perdue (voir [Sch01]).

Démosthène (˜384 av. J.C., ˜322 av. J.C.) écrit ([227] et [229]) que nous avons besoin d'utiliser des cailloux pour effectuer les calculs qui sont trop difficiles à faire à la main.

Hérodote [II 36] écrit à propos des Égyptiens : "*Ils écrivent leurs caractères et calculent avec des cailloux, de droite à gauche là où les Grecs le font de gauche à droite*".

Le vase grec dit de Darius, trouvé en 1851 et maintenant conservé au musée de Naples, montre un trésorier tenant une tablette à la main alors qu'il semble manipuler des compteurs sur une table avec l'autre (figure 1.5, voir aussi une photo dans [Smi25], vol. II, p. 161).

Une table d'abaque a été trouvée dans l'île de Salamis près du Pirée (figure 1.6).

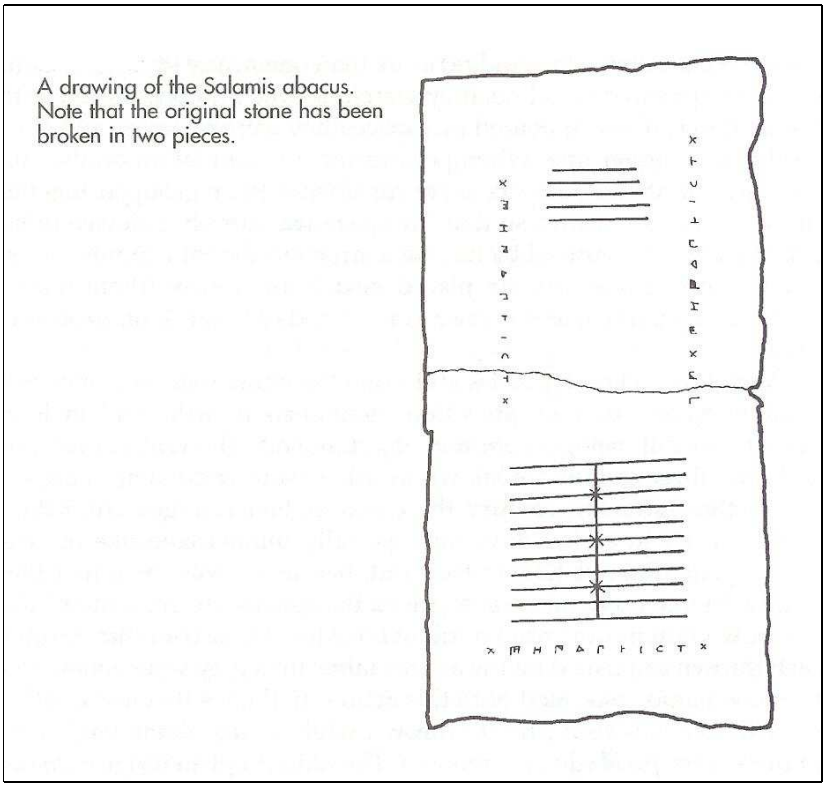


Fig. 1.6 – Abaque de Salamis ([Wil85], p. 57)

On sait que la manipulation des cailloux sur de la poussière, ou l'utilisation d'un doigt ou d'un stylet sur de la poussière fine ou du sable déposé sur une table, est utilisée depuis les temps les plus anciens. Le mot sémite *abaq* (poussière) semble être à l'origine du mot *abaque*. Les Grecs utilisaient le mot *abax* pour désigner une surface plane sur laquelle ils effectuaient leurs calculs. Le terme *abaque* a désigné plusieurs choses au cours de son histoire, y compris les bouliers au XIX^e et XX^e siècles.

1.3.2 Naissance des calculatrices

On appelle **calculatrice** *toute machine permettant d'effectuer rapidement l'une ou la totalité des quatre opérations : addition, soustraction, multiplication, division. Il s'agit en général d'opérations sur les entiers mais aussi quelquefois sur les*

nombres à virgule.

Un bon résumé de l'histoire des calculatrices se trouve dans le livre *A history of Computing Technology* [Wil85] de Michael WILLIAMS, avec des références bibliographiques. Nous nous nous contenterons ici d'en rappeler les grandes étapes.

On sait que la détermination des impôts donne lieu à la naissance de la première machine à calculer mécanique de Blaise PASCAL (1623–1662) en 1642. En fait celui-ci a été devancé par Wilhem SCHICKARD (1592–1635), qui a certainement construit une calculatrice permettant les additions en 1623, mais qui est perdue. Gottfried Wilhem LEIBNIZ (1646–1716) construisit une machine capable d'effectuer des multiplications en 1670. De toute façon aucune de ces machines n'a connu le succès commercial escompté ; elles ne furent produites qu'en quelques exemplaires.

La première calculatrice commerciale, inspirée de la machine de Leibniz, fut l'*arithmomètre* de THOMAS de Colmar, mise sur le marché en 1820 et qui fut vendu jusqu'à la première guerre mondiale. D'autres machines, toutes mécaniques, furent commercialisées jusqu'au début des années 1970. Elles furent alors remplacées par des calculettes électroniques, sous-produit des ordinateurs.

1.3.3 Machines dédiées

On appelle **machine dédiée** *un outil d'aide aux calculs capable d'effectuer des calculs plus compliqués que les quatre opérations sans être une machine universelle.*

Il s'agit d'abord de *calculateurs analogiques* (et non numériques), tels que ceux qui servent à la prévision des marées (en particulier celui de lord KELVIN), qui sont décrits dans la première partie de [Gol72]. Il s'agit ensuite de calculateurs mécaniques tels que la machine Z1 de Konrad ZUSE (1910–1995), des machines à relais de Georges STIBITZ aux établissements Bell (Model I à Model VI) construites à partir de 1937, des machines de Harvard de Howard AIKEN (Mark I à Mark IV) et des premiers calculateurs IBM. Viennent enfin les calculateurs électroniques telles que la machine ABC de John ATANASOFF (1903–1995) et Clifford BERRY (1918–1963) construite à partir de 1939 et surtout l'ENIAC de l'université de Pennsylvanie. Une première description de ces machines se trouve dans [Wil85]

1.3.4 Machines universelles ou ordinateurs

On appelle **machine universelle***, ou* **ordinateur***, tout outil d'aide aux calculs capable d'effectuer tout calcul qui le serait par une machine quelconque.*

Comme nous l'avons vu ci-dessus, le premier ordinateur (non construit) est la *machine analytique* de Charles BABBAGE (1791–1871), entièrement mécanique. L'idée du premier ordinateur, due essentiellement à John VON NEUMANN est l'EDVAC conçu en 1945. Mais à cause des dissensions au sein de l'équipe, il ne sera terminé qu'après l'EDSAC de Cambridge en Angleterre, qui date de 1950. On pourra trouver une introduction à la naissance des ordinateurs, avec des références bibliographiques, dans [Wil85].

Vint ensuite la commercialisation des ordinateurs, avec la toute puissance d'IBM durant une période, puis l'apparition des micro-ordinateurs.

1.3.5 Programmation des ordinateurs

Puisque, d'une part, les ordinateurs sont capables d'effectuer tous les calculs qu'une autre machine peut effectuer et que, d'autre part, de tels calculs sont en nombre infini, il faut un moyen de spécifier le calcul à effectuer. Ceci est d'ailleurs déjà vrai de certaines machines dédiées. On parle de **programme**. Les premiers programmes correspondaient à un câblage sur la façade arrière de l'ordinateur ;

cela pouvait prendre trois jours aux techniciens pour un algorithme relativement simple. L'idée fondamentale de John VON NEUMANN est d'enregistrer le programme auusi bien que les données. Au départ on utilise ce qui sera appelé plus tard le *langage machine* avec des 0 et des 1. On comprend que la tâche de programmation revient alors à des ingénieurs bien formés. Les *langages d'assemblages*, avec des mnémonymes pour les noms des opérations primitives permettent d'arranger un peu la situation. L'apparition des *langages évolués*, FORTRAN et COBOL en 1957, simplifient nettement la tâche de la programmation. De nombreux langages évolués apparaissent ensuite (ALGOL, PASCAL, C, ADA, C++, Java...).

On prend l'habitude à partir de 1957 de présenter les algorithmes dans de tels langages de programmation, ou dans des *pseudo-langages* proches de ceux-ci. Mais nous allons voir que ceci ne permet pas de présenter tous les algorithmes, ce dont on ne prendra vraiment conscience qu'à la fin des années 1980.

1.4 Problèmes calculables

1.4.1 Premiers doutes sur les limites des calculs par programme

Apparaissent de plus en plus de programmes de calculs. Non pas, historiquement, les programmes d'ordinateur mais les programmes dans les bureaux de calculs. Deux problèmes, cependant, vont inciter à s'interroger sur les limites de ceux-ci.

Attitude générale.- Pendant longtemps les mathématiciens ont résolu des problèmes particuliers par des méthodes générales, des méthodes souvent plus générales que ce pourquoi elles ont été trouvées. On s'interroge, par exemple, sur la contenance d'un tonneau de telle forme. La méthode la plus générale de l'Antiquité, la *méthode d'exhaustion*, consiste à deviner la formule pour le volume puis à la démontrer en approximant par des polyèdres de plus en plus proches. Au XVII^e siècle, la méthode du calcul intégral de NEWTON et LEIBNIZ permet de calculer les volumes sans avoir d'idée *a priori* sur le résultat. À aucun moment, cependant, on ne s'interroge sur la notion générale de volume.

Le XIX^e siècle va être un siècle à la fois de rigueur et de classification. On ne s'intéresse plus à tel ou tel problème particulier, on veut formuler le cas général et obtenir des théorèmes généraux sur celui-ci.

Premier problème : théorie des invariants.- Considérons une courbe algébrique dans le plan, une surface dans l'espace ou une variété dans un espace de dimension arbitraire représentée par une équation polynomiale. Lorsqu'on change de repère, l'équation de la courbe change mais on peut mettre en évidence sur l'équation des propriétés invariantes par rapport à un changement de repère. Ces invariants traduisent les propriétés géométriques intrinsèques de la courbe.

Une *variété algébrique* est définie, dans un repère donné, par $P(x_1, ..., x_n) = 0$, où P est un polynôme homogène de degré m. Un *invariant* est un polynôme I en les coefficients des polynômes homogènes à n variables de degré m tel que pour toute transformation linéaire, de déterminant 1, on ait $I(a) = I(a')$, si a est la liste des coefficients de P et a' celle de l'équation P' après la transformation. Le problème consiste à déterminer les invariants de la variété algébrique.

En 1868, GORDAN détermine les invariants des courbes du plan. Pendant vingt ans, personne ne réussit à améliorer ces résultats. En 1890, David HILBERT donne une réponse en dimension quelconque, en montrant que, dans un espace de dimension donnée, il existe une famille finie qui engendre l'ensemble des invariants par des

opérations simples (*Théorème de la base de Hilbert*). Cependant la démonstration ne donne pas de procédure pour calculer la famille génératrice. Cette voie abstraite rencontre une vive opposition. GORDAN déclare : "Ce n'est pas des mathématiques, c'est de la théologie". HILBERT reprend le problème et, en 1893, réussit à donner une démonstration constructive qui permet de calculer la famille génératrice des invariants.[5]

C'est certainement la première fois que l'on insiste sur l'effectivité ou calculabilité d'un problème.

Deuxième problème : l'axiome du choix.- Les mathématiques des XVII^e et XVIII^e siècles sont fortement liées à la physique. Cette dernièrela physique a besoin de résoudre des équations différentielles. Pour les cas simples, on a pu trouver des solutions exactes à certaines d'entre elles. Au XIX^e siècle, on commence à comprendre que l'on n'a pas toujours de *solution analytique* exacte, c'est-à-dire exprimable à partir de fonstions connues. Le calcul des valeurs approchées de la solution en un certain nombre de points est suffisant pour les physiciens et les ingénieurs. Encore faut-il disposer de théorèmes sur certaines propriétés générales. Augustin CAUCHY, avec des hypothèses précisées par LIPSCHITZ, montre l'existence et l'unicité de la solution d'une équation différentielle avec des conditions initiales données, ce qui reflète bien l'expérience physique.

Guiseppe PEANO améliore le résultat de CAUCHY en montrant l'existence dans le seul cas de la continuité, mais sans unicité comme le montre l'exemple classique $y' = \sqrt[3]{x}$.

On s'aperçoit rapidement que PEANO utilise implicitement une hypothèse pour démontrer son résultat, hypothèse qui va être connue sous le nom d'*axiome du choix*. Un énoncé simple de l'axiome du choix dit que le produit cartésien (infini) d'ensembles non vides est un ensemble non vide. Émile BOREL s'interroge sur la notion d'effectivité à propos de la justification de l'axiome du choix dans ses *Leçons sur les fonctions* de 1898 [Bor98].

1.4.2 Retour en arrière : émergence des problèmes de possibilité

Au dix-neuvième siècle naît une nouvelle façon de répondre aux problèmes, le type de réponse étant inattendu pour un mathématicien de l'époque. Jusqu'alors, lorsqu'on posait un problème on s'attendait à ce qu'il soit résolu tôt ou tard, sous la forme sous laquelle il était posé. Le nouveau type de réponse est : *il n'existe pas de réponse au problème sous la forme sous laquelle il est posé*. Cette nouvelle façon de répondre apparaît à propos de problèmes anciens sur la résolution des équations algébriques et sur le problème des constructions à la règle et au compas.

Le premier exemple en est donné par RUFFINI en 1799 [Ruf04]. Les équations algébriques sont apparues pour des raisons diverses (non vraiment explicitées) très tôt. La résolution des équations du second degré date de la Mésopotamie ancienne, comme nous l'avons vu ci-dessus. La résolution des équations du troisième et du quatrième degré date du XVI^e siècle (TARTAGLIA, FERRARI ...). On cherche alors activement à résoudre l'équation du cinquième degré, plus exactement par radicaux. RUFFINI montre en 1799 que c'est impossible, ou tout au moins l'affirme puisque son article est considéré comme incompréhensible. Qu'importe puisque les démonstrations d'ABEL (en 1824) puis le théorème plus général d'Évariste GALOIS en 1832 (indiquant dans quel cas une équation algébrique est résoluble par radicaux) confirmeront ce résultat.

[5] Pour une introduction à l'œuvre de David HILBERT, on pourra se reporter au petit livre [CN01].

Le second problème concerne les constructions géométriques à l'aide de la règle et du compas. L'Antiquité laisse trois problèmes non résolus à cepropos : la duplication du cube (en terme moderne il faut construire la racine cubique de 2), la trisection d'un angle quelconque (la construction de la bissectrice est connue depuis longtemps) et la quadrature du cercle (étant donné le rayon d'un cercle, autrement dit un segment de droite, construire le côté, un autre segment, d'un carré ayant même aire que le cercle). WANTZEL montre en 1837 [Wan37] qu'il est impossible de résoudre les deux premiers problèmes : les longueurs des segments constructibles à l'aide de la règle et du compas par rapport à un segment de longueur un sont appelés les *nombres constructibles* ; WANTZEL commence par montrer que les nombres constructibles sont ceux des extensions quadratiques itérées du corps des rationnels ; il montre ensuite que ni $\sqrt[3]{3}$, ni $sin(10^o)$ ne sont des nombres constructibles. LINDEMANN [Lin82] montre l'impossibilité de la quadrature du cercle en 1882 en démontrant que le nombre π est transcendant.

Beaucoup d'autres solutions de ce type apparaissent. David HILBERT y fait référence dans son célèbre exposé *Sur les problèmes futurs des Mathématiques* de 1900 :

> *Il se peut aussi que l'on s'efforce d'obtenir une solution en se basant sur des hypothèses insuffisantes ou mal comprises et que, par suite, on ne puisse atteindre le but. Il s'agit alors de démontrer l'impossibilité de résoudre le problème en se servant d'hypothèses telles qu'elles ont été données ou interprétées. Les Anciens nous ont donné les premiers exemples de pareilles démonstrations d'impossibilité ; ils ont démontré ainsi que dans un triangle rectangle isocèle l'hypoténuse et le côté de l'angle droit sont dans un rapport irrationnel. Dans les Mathématiques contemporaines, la question de l'impossibilité de certaines solutions joue un rôle prépondérant ; c'est à ce point de vue de la démonstration de l'impossibilité que d'anciens et difficiles problèmes, tels que ceux de la démonstration de l'axiome des parallèles, de la quadrature du cercle et de la résolution par radicaux de l'équation du cinquième degré, ont reçu une solution parfaitement satisfaisante et rigoureuse bien qu'en un sens tout différent de celui qu'on cherchait primitivement. Le fait remarquable dont nous venons de parler et certains raisonnements philosophiques ont fait naître en nous la conviction que partagera certainement tout mathématicien, mais que jusqu'ici personne n'a étayée d'aucune preuve, la conviction, dis-je, que tout problème mathématique déterminé doit être forcément susceptible d'une solution rigoureuse, que ce soit par une réponse directe à la question posée, ou bien par la démonstration de l'impossibilité de la résolution, c'est-à-dire de l'insuccès de toute tentative de résolution.*
>
> [Hil00], p. 11–12.

Il est d'ailleurs curieux que, alors qu'il ait bien conscience de solutions inattendues, HILBERT ne remette absolument pas en doute les possibilités du calcul. L'une des preuves les plus flagrantes de cette dernière affirmation est l'analyse faite par Yuri MATIIASSEVICH en 1999 de la façon dont David HILBERT pose son dixième problème (sur les mathématiques futures) en 1900 :

> *Le dixième problème occupe moins d'espace qu'aucun autre problème dans l'article de Hilbert. Durant son exposé il n'en dit pas un mot, ainsi que sur quelques autres problèmes. Son exposé dura deux heures et demi mais ceci ne fut pas suffisant pour présenter les vingt-trois problèmes ; ainsi quelques problèmes, dont le dixième, ne furent pas présentés oralement mais seulement inclus dans la version imprimée de l'exposé.*

> *Ainsi Hilbert ne donna-t-il pas de motivation pour le dixième problème. Nous pouvons seulement deviner pourquoi il ne parla que des solutions en "entiers rationnels". Nous avons vu que cela est équivalent à rechercher un algorithme pour résoudre les équations diophantiennes en entiers naturels. Mais, en fait, Diophante lui-même ne résolvait les équations ni en entiers naturels, ni en entiers relatifs, il cherchait des solutions rationnelles. Donc pourquoi Hilbert ne demanda-t-il pas une procédure pour déterminer l'existence de solutions rationnelles ? La réponse est plus ou moins évidente. Hilbert était optimiste et croyait en l'existence d'un algorithme pour résoudre les équations diophantiennes en entiers. Un tel algorithme nous permettrait également de résoudre les équations en rationnels.*
>
> [Mat99], p. 297

Bien sûr on ne peut en déduire *a priori* que c'est uniquement pour un problème particulier qu'Hilbert ne se pose pas la question de la calculabilité. Mais en fait aucun des problèmes ne porte sur la calculabilité.

1.4.3 Le besoin de caractériser les fonctions calculables

Nous avons vu ci-dessus survenir quelques doutes sur la calculabilité de certaines opérations, en particulier par Émile Borel mais sans qu'il y ait de définition de ce qui est calculable. La nécessité de définir rigoureusement la *calculabilité* d'une fonction se fera ressentir à propos de deux problèmes.

Le problème de la décidabilité de l'arithmétique élémentaire.- Vous vous souvenez sans doute des problèmes de Géométrie qu'il a rencontrés au Lycée. Il faut, suivant la capacité de chacun, plus ou moins de temps pour les résoudre. Certains sont même si difficiles qu'il fallait attendre la solution du professeur. D'autres, encore plus difficile, faisaient l'objet d'énoncés dans des revues telle que feue la *Revue de Mathématiques Élementaires* en France.

Alfred Tarski montre à la fin des années 1920 (mais publié tardivement [Tar48, Tar51]) qu'en fait il n'y a nul besoin de créativité pour résoudre ces problèmes. On peut automatiser la géométrie élémentaire, c'est-à-dire que l'on peut constuire une machine à laquelle on donne l'énoncé et celle-ci en donne le résultat. Il s'agit d'un résultat théorique, la machine n'étant pas construite à l'époque. Ce n'est que dans les années 1970 qu'elle commencera à apparaître comme programme d'ordinateur.

Puisque la géométrie élémentaire est automatisable, il doit bien en être également ainsi de l'arithmétique élémentaire, se dit-on à l'époque. Des recherches sont alors effectuées dans ce sens, mais on s'aperçoit rapidement que le cas est plus coriace. On commence même à se dire qu'il ne doit pas en être ainsi. Mais comment le démontrer ? Et d'abord comment démontrer qu'un problème n'est pas automatisable. Il faudrait déjà préciser ce qu'est un problème automatisable.

Le théorème d'incomplétude de Gödel.- En 1931, Kurt Gödel répond à Hilbert ("*la conviction, dis-je, que tout problème mathématique déterminé doit être forcément susceptible d'une solution rigoureuse, que ce soit par une réponse directe à la question posée, ou bien par la démonstration de l'impossibilité de la résolution, c'est-à-dire de l'insuccès de toute tentative de résolution*") par son célèbre théorème d'incomplétude : *quelle que soit la théorie mathématique considérée, il existe un énoncé du langage de celle-ci qui ne peut ni être démontré, ni réfuté dans cette théorie.*

Gödel [Göd31] a besoin d'un minimum d'hypothèses sur ce qu'est une théorie mathématique pour démontrer son théorème. Une théorie mathématique est une

théorie logique du premier ordre, avec un certain ensemble d'axiomes. Dans ce contexte l'ensemble des axiomes ne peut pas être fini mais on doit savoir si un énoncé du langage de la théorie est un axiome ou non. Autrement dit on doit pouvoir décider si c'est un axiome.

Pour démontrer son théorème, GÖDEL donne lui-même une définition de ce qu'est une fonction calculable, inspirée de Jean HERBRAND. Il ne sera cependant convaincu qu'il a bien ainsi appréhendé la notion de fonction calculable qu'à l'apparition du modèle de Turing en 1936 (et l'équivalence avec son modèle).

1.4.4 Caractérisation des fonctions calculables

Sous la direction de NEUMANN, Alan TURING passe de la théorie des groupes à l'hypothèse de Riemmann et, pour cela, au calcul des zéros de la fonction dzêta. Les moyens théoriques sont hors de portée ; il s'agit donc d'effectuer des calculs sur les décimaux (avec les erreurs inhérentes) pour obtenir des résultats sur les réels.

Il abandonne ce problème pour une réflexion globale sur les réels qui peuvent être calculables et plus généralement sur "ce qui est calculable". Il répond à la question en 1936 [Tur36] en définissant son célèbre modèle de machines abstraites. Sa réponse est immédiatement acceptée. La même année Alonzo CHURCH [Chu36] clame que toute notion de calculabilité est réductible aux machines de Turing (ce qui est connu sous le nom de *thèse de Church*).

Plusieurs autres modèles de calculabilité sont proposés, dont on montre facilement qu'ils sont tous équivalents à celui des machines de Turing.

1.4.5 Applications de la thèse de Church

Les applications de la thèse de Church n'aident en rien les calculs. Elle montre seulement que, dans certains cas, il est inutile de perdre son temps à essayer de trouver un algorithme, puisqu'il n'en existe pas. C'est ainsi que l'on sait démontrer rigoureusement qu'il n'existe pas de programme d'ordinateur qui prendrait en entrée un programme (par exemple écrit en langage C) et qui dirait si ce programme s'arrête toujours ou peut boucler sur certaines données. De même, au grand dam des enseignants, il n'existe pas de programme qui prendrait en entrée, à propos d'un problème de programmation, le corrigé de l'enseignant et la solution proposée par l'étudiant et qui dirait si ces deux programmes font la même chose.

On peut également enfin démontrer que l'arithmétique élémentaire, *a contrario* de la géométrie élémentaire, est indécidable.

1.4.6 Les langages Turing-complets

Certaines machines electro-mécaniques ou electroniques ont été conçues pour résoudre tel ou tel problème particulier (par exemple le calcul des coefficients de marée). De nos jours, ces machines ont été avantageusement remplacées par un ordinateur faisant tourner en permanence le même logiciel : c'est le cas de la GTC (*Gestion Technique Centralisée*) mais aussi des agendas électroniques ou même de certains ordinateurs portables. En effet on se sert de la versalité des microprocesseurs/micro-contrôleurs alliés à un système d'exploitation pour gagner beaucoup de temps lors de la phase de développement.

Par ailleurs il existe des langages de programmation spécialisés dont le but n'est pas de programmer tous les calculs possibles : voir ABEL et VHDL pour la conception des circuits logiques, TEX pour le traitement de textes et autres. On n'est pas capable de calculer toute fonction calculable avec de telles machines ou de tels langages.

On dit qu'un **langage** *(de programmation) est* **Turing-complet** *s'il permet de calculer toute fonction calculable.*

À proprement parlé, il n'existe aucun langage de programmation Turing-complet. Prenons le cas du langage C par exemple. Les structures de contrôle (séquencement, test et itérations) sont suffisantes. Le problème provient de ce qu'il n'existe aucun type primitif dénotant un ensemble infini. Le type `int` des entiers, par exemple, ne dénote que les entiers compris entre -2^N et $2^N - 1$ pour un N plus ou moins grand suivant l'implémentation de ce langage. Bien entendu on peut parler de "grands" entiers, par exemple en considérant des listes chaînées d'entiers, mais on obtient là encore qu'un nombre fini d'entiers.

D'un point de vue pragmatique, un langage sera dit **quasi-Turing-complet** *s'il permet de calculer toute fonction calculable si son type élémentatire d'entiers dénotait tous les entiers.*

1.5 Vers une définition des algorithmes

1.5.1 Au-delà de la thèse de Church

L'avancée extraordinaire d'Alan Turing apporte un cadre définitif pour aborder de nombreux problèmes, en particulier ceux dit de décidabilité et d'indécidabilité. Il ne s'agit évidemment pas de la panacée cependant : elle apporte un cadre de première approximation pour d'autres problèmes, sans permettre de les résoudre totalement. On a alors besoin d'aller au-delà de la seule formalisation de ce qui est calculable pour les résoudre complètement.

Le premier type de problèmes pour lequel le cadre laissé par Turing n'est pas suffisant concerne le calcul des ressources nécessaires pour calculer une fonction lorsque celle-ci est calculable. Les deux ressources essentielles sont le temps de calcul et la taille des résultats intermédiaires (appelé l'*espace* par convention). L'étude de l'utilisation de ces deux ressources a conduit à la *théorie de la complexité algorithmique* dans les années 1960. Le problème non résolu le plus célèbre est celui de P = NP.

Le second type de problèmes pour lequel le cadre laissé par Turing n'est pas suffisant est celui qui consiste, lorsqu'une fonction est calculable, à distinguer les algorithmes proposés pour la calculer. Ceci conduit à la nécessité, si ceci est possible mais rien ne permet de l'affirmer *a priori*, de dégager un langage universel de présentation des algorithmes.

C'est à ce dernier type de problèmes que nous allons nous intéresser dans ce livre.

1.5.2 Algorithmes et langages Turing complets

1.5.2.1 Écriture des algorithmes

Pour une même fonction calculable, il existe plusieurs méthodes pour la calculer. Le tri de données est certainement le problème qui a donné lieu au plus grand nombre de méthodes de résolution par calcul (tri sélection, tri par insertion, tri à bulle, tri fusion, tri rapide, tri Shell...). Techniquement disons que, pour une fonction calculable, il existe plusieurs *algorithmes* qui conduisent au résultat.

Pour qu'un langage de programmation soit qualifié de Turing-complet, il suffit que, pour toute fonction calculable, il existe au moins un algorithme permettant de la calculer qui soit implémentable dans ce langage. Bien entendu, beaucoup d'algorithmes sont implémentables. Les différentes méthodes de tri sont plus ou

moins implémentables sur les langages de programmation courant, sinon cela se saurait.

Une question se pose cependant :

Tout algorithme peut-il s'écrire dans un langage Turing-complet donné ?

La première réaction à cette question est certainement de répondre positivement, en disant que cela se saurait s'il en était autrement. Curieusement nous allons voir que, cependant, la réponse est non. Nous avons du mal à nous en apercevoir car, si on ne peut pas écrire exactement les algorithmes, on peut en général les émuler sous une forme assez proche.

1.5.2.2 L'exemple de l'échange

Considérons l'exemple classique de l'échange de deux données, ou plus exactement des valeurs de deux variables `a` et `b`. L'algorithme au sens intuitif se décrit correctement sous la forme suivante :

```
a := b
b := a
```

ce que fait d'ailleurs tout néophyte en programmation. On fait rapidement remarquer à un tel néophyte que ceci ne convient pas avec les langages de programmation habituels et on lui apprend à écrire un programme correct sous une forme proche, en recourant à quelques astuces. Soit on utilise une variable intermédiaire :

```
c := a
a := b
b := c
```

soit, dans le cas des entiers naturels, on utilise l'addition et la soustraction :

```
a := a + b
b := a - b
a := a - b
```

Remarquons que, dans aucun des deux cas, il ne s'agit de l'algorithme initial. Il s'agit seulement d'une variante proche de celui-ci :

- Dans le premier cas, on utilise une variable supplémentaire par rapport à l'algorithme intuitif.
- Dans le second cas, on utilise des opérations qui semblent éloignées de la nature du problème.
- Dans les deux cas on utilise trois instructions au lieu des deux instructions nécessaires pour la présentation de l'algorithme intuitif. Il n'y a pas traduction pas à pas : on a trois pas au lieu de deux.

L'analyse de nombreux algorithmes et de la façon dont ils sont programmés montre que ce phénomène est courant. L'une des difficultés des enseignants de programmation ou d'algorithmique consiste à faire substituer des algorithmes naturels par des variantes qui s'écrivent dans le langage de programmation utilisé. Une série de trucs et d'astuces est acquise au fur et à mesure du déroulement du cours.

1.5.3 Définition informelle d'un algorithme

Qu'est-ce qu'un algorithme ? Il n'existe pas réellement de définition satisfaisante jusqu'à celle donnée par Yuri Gurevich. Citons par exemple les présentations proposées par deux éminents spécialistes à la fin des années 1960 :

L'idée d'un algorithme ou d'une procédure effective apparaît lorsque nous sommes en présence d'un ensemble d'instructions pour savoir comment se comporter. Ceci arrive lorsque, au cours du travail sur un problème, nous découvrons qu'une certaine procédure, si elle est exécutée proprement, finira en nous donnant la réponse. Une fois que nous avons fait une telle découverte, la tâche pour trouver la solution est réduite d'un effort intellectuel à un effort simple ; de découvrir la procédure à obéir aux instructions spécifiées.

Mais comment dire, étant donné ce qui apparaît être un ensemble d'instructions, ce que nous avons réellement à faire ? Comment pouvons-nous être sûr que nous agissons effectivement ainsi, en accord avec les "règles", sans jamais avoir à faire un choix de plus ou une innovation de notre propre fait ?

[...]

La position que nous prendrons est celle-ci : si la procédure peut être réalisée par une machine simple, de telle façon qu'il ne puisse être question ou de nécessité d'"innovation" ou d'"intelligence", alors nous pouvons être sûr que la spécification est complète et que nous avons une "procédure effective". Nous ne nous battrons pas contre cela.

[Min67], p. 105, notre traduction.

La signification moderne d'algorithme est assez similaire à celle de recette, processus, méthode, technique, procédure, routine, à part que le mot "algorithme" connote quelque chose de légèrement différent. Étant simplement un ensemble fini de règles qui donne une suite d'opérations pour résoudre un type spécifique de problèmes, un algoritme a cinq caractéristiques importantes :

1. *Finitude. Un algorithme doit toujours se terminer après un nombre fini d'étapes [...]*
2. *Défini. Chaque étape d'un algorithme doit être définie précisément ; les actions à effectuer doivent être rigoureusement spécifiées de façon non ambiguë pour chaque cas [...]*
3. *Entrées. Un algorithme a zéro ou plus d'entrées, c'est-à-dire des quantités qui lui sont données initiallement avant que l'algorithme commence. Ces entrées sont prises dans des ensembles spécifiés d'objets [...]*
4. *Sorties. Un algorithme a zéro ou plus de sorties, c'est-à-dire des quantités qui ont une relation spécifiées avec les entrées [...]*
5. *Effectivité. On s'attend en général à ce qu'un algorithme soit effectif. Ceci signifie que toutes les opérations qui doivent être effectuées dans l'algorithme doivent être suffisamment basiques pour qu'elles puissent l'être en principe exactement et en un temps fini par un homme utilisant du papier et un crayon [...]*

[Knu68], p. 4, notre traduction.

Nous avons la notion intuitive d'algorithme sans posséder de définition formelle. On peut dire qu'un algorithme va s'écrire, en langage vernaculaire, en pseudo-code ou en langage de programmation comme une instruction composée, formée d'instructions élémentaires et de structures de contrôle. Le jeu des instructions élémentaires et des structures de contrôle dépend du langage de programmation utilisé pour exprimer l'algorithme.

1.5.4 Les langages algorithmiquement complets

On se retouve dans la situation des années 1930 où on disposait de nombreux outils d'aides au calcul et où on se posait la question d'une machine universelle :

Existe-t-il une machine capable de calculer toute fonction calculable sur au moins une machine ?

La réponse fut donnée en deux étapes : d'abord la présentation d'un modèle universel (les machines de Turing) puis la réalisation des premiers ordinateurs.

La question est maintenant la suivante :

> *Existe-t-il un langage de présentation des algorithmes qui permette de présenter tout algorithme écrit en n'importe quel langage avec le même nombre d'étapes d'exécution (on dit pas à pas) ?*

On ne peut pas, bien sûr, retenir toutes les instructions élémentaires et toutes les structures de contrôle de tous les langages de programmation présent et à venir. Outre le capharnaüm que cela engendrerait, on se retrouverait devant un nombre infini d'instructions élémentaires et un nombre infini de structures de contrôle.

Un langage est **algorithmiquement complet** *s'il permet d'écrire pas à pas tout algorithme.*

On parle aussi d'**UAM** pour *Univeral Algorithmic Machine* (on peut aussi remplacer *Machine* par *Model*).

1.5.5 La réponse de Yuri Gurevich

Remarquons d'abord que les machines de Turing ne sont pas des UAM. Toute fonction calculable possède un programme la calculant exprimable comme machine de Turing. Il existe cependant des algorithmes qui ne sont pas exprimables directement comme machine de Turing, ils sont seulement **émulables**. Nous avons vu à propos de l'échange qu'aucun langage de programmation actuel n'est algorithmiquement complet, il y a émulation mais pas émulation pas à pas.

Kolmogorov et Uspenky publient en 1958 un article dans lequel est présenté ce qui peut être considéré comme un essai de définition de machine algorithmiquement complète [KU58], mais dans lequel n'apparaît aucune réflexion globale, aucun aspect philosophique. À la mort de Kolmogorov, Yuri Gurevich a écrit un article [Gur88] dans lequel il indique que Kolmogorov aurait pu poser ce problème des langages algorithmiquement complets : "chaque calcul, utilisant seulement une action locale restreinte à chaque instant, peut être vu comme le calcul (pas seulement une simulation, mais vraiment un calcul) d'une machine KU appropriée". Un peu plus tard, Uspensky répond dans un article de la revue *The Journal of Symbolic Logic* : "*Je pense que Yuri Gurevich avait une bonne idée, un nouvel éclairage sur notre article.*" [Usp92].

La notion est dégagée mais le modèle n'est pas satisfaisant. Yuri Gurevich critiquera ce modèle et proposera son propre modèle, sous des noms variés (allant de *evolving algebras* à *ASM* pour *Abstract State Machine*). Il défendra ce qu'on peut appeler la **thèse de Gurevich** (la notion d'algorithme est entièrement appréhendée par son modèle) à la fin des années 1990. Les ASM apparaissent dans [Gur84] (sous le nom de "*dynamic structures*"). Un an plus tard, il reprend dans une note :

> *Premièrement, nous adaptons la thèse de Turing au cas où seules des machines avec des ressources bornées sont considérées. Deuxièmement,*

nous définisson un type plus général d'outils de calculs abstraits, appelés structures dynamiques, et nous posons la nouvelle thèse suivante : chaque outil de calcul peut être simulé par une structure dynamique appropriée – d'à peu près la même taille – en temps réel ; une famille uniforme d'outils de calculs peut être simulée uniformément par une famille appropriée de structures dynamiques en temps réel. En particulier, tout outil de calcul séquentiel peut être simulé par une structure dynamique séquentielle appropriée.

[Gur85]