Les langages numériques

Jean Vuillemin

Ecole Normale Supérieure
45 rue d'Ulm, Paris 75230 cedex 05.

Résumé : *L'histoire des numérations montre que l'homme a utilisé une grande variété de systèmes pour écrire ses nombres. Pourtant, les représentations des nombres sur les abaques de calcul semblent presque toutes fondées sur le système décimal ou ses variantes simples, depuis la plus haute antiquité. L'écriture décimale qui en résulte ne naît pourtant qu'au IX*^{e} *siècle, en Inde ; elle est aujourd'hui la première partie universelle des langues de l'homme.*

Depuis cinquante ans, l'âge de l'information nous impose le système binaire pour stocker les nombres, les calculer et les transmettre. Les raisons de ce choix unique viennent autant des mathématiques que de la physique et l'informatique. Le langage binaire permet de représenter les nombres, mais aussi les textes, les images et les sons - toutes les formes numériques de l'information. La technologie des réseaux d'ordinateur fait aujourd'hui du binaire la langue de communication la plus universelle et utilisée dans le monde - encore bien plus que le système décimal.

D'après un haut relief de Saqqara en Egypte. Les oiseaux indiquent *l'ordre de lecture*, de droite à gauche avec le bec au vent. Les autres hiéroglyphes *comptent* les tributs de Pharaon après une campagne victorieuse. Chaque signe vaut une puissance de dix : un pour la barre, 10 pour le fer à cheval, 100 pour le serpent, 1 000 pour le lotus, 10 000 pour l'obélisque et 100 000 pour la salamandre. Les quatre nombres qui figurent ici s'écrivent donc, en décimal, 11 110 (haut gauche), 121 200 (haut droit), 111 200 (bas gauche) et 121 022 (bas droit).

Figure I : Nombres hiéroglyphes.

1. Numérations antiques

L'histoire des numérations écrites est longue est variée ; lire [1] et [2] qui font autorité en ce domaine. La base 10 est la plus commune - Egypte, Inde, Chine ; les Mayas d'Amérique utilisaient la base 20 ; les civilisations de Sumer et Babylone se servaient de la base 60 ; il nous en reste partie de nos mesures du temps, et des angles.

Dans les numérations *alphabétiques* - Egypte, Grèce, Chine - chaque symbole a une valeur numérique fixe et indépendante de sa position dans le nombre. L'ordre d'écriture des chiffres n'a alors pas d'importance, et on a pas besoin d'une notation explicite pour le zéro. Observez pourtant que les hiéroglyphes de la fig. I sont proprement alignés, comme dans toute *numération décimale de position*, et comme sur tout abaque de calcul.

Dans les numérations de position - Babylone, Inde, Maya - la valeur d'un symbole est multipliée par une puissance de la base ; son exposant est donné par la position du symbole dans le nombre. Il faut donc une représentation explicite du zéro pour marquer la position d'une colonne vide. Un simple espace est la façon la plus naturelle de marquer le zéro. L'écriture explicite du symbole 0 évite toutes les ambiguïtés de lecture que l'on trouve en utilisant l'espace, caractère invisible. Cette écriture n'apparaît pourtant que beaucoup plus tard en Inde – fig. III – puis en Chine – fig. VII. A notre sens, l'apparition du zéro explicite – qui remplace le zéro marqué implicitement par un espace - est une adaptation naturelle de la représentation des nombres à la technologie – alors naissante – de l'écriture manuscrite bon marché. Nous n'y voyons pas la révolution scientifique que certains [5] accordent à la naissance du symbole 0.

1.1. Babylone

Cette tablette - d'après YBC 7289, collection babylonienne de Yale - présente trois nombres écrits à la plume - on dit *cunéiforme* - sur une argile cuite, il y a près de 4000 ans. C'est table des valeurs de 1/2, $\sqrt{2}$ et $1/\sqrt{2}$, avec une précision équivalente à six chiffres décimaux qui est supérieure à celle de bien des mesures de la physique moderne.

Figure II : Tablette babylonienne.

Les numérations de Sumer et Babylone sont *sexagésimales* - base 60. Les chiffres sont écrits avec deux symboles : encoche avec la plume verticale pour les unités, horizontale pour les dizaines. Ainsi, le chiffre en haut à gauche de la fig. II vaut 30. Le nombre du centre est formé de la suite de chiffres *sexagésimaux* [1 24 51 10] et celui du bas [42 25 35], en lisant de gauche à droite des chiffres forts vers les chiffres faibles.

Soulignons que les nombres de Babylone s'écrivent avec seulement deux symboles, comme le binaire alors que la base est 60. Il convient d'y ajouter l'espace, qui sert à marquer le zéro - avec toutes les ambiguïtés de lecture qu'une telle convention peut amener. L'espace sert aussi à marquer la position du point fractionnaire ; faute de cette marque, on doit reconstruire sa position d'après le sens des valeurs trouvées ; il est heureusement bien clair ici.

Pour interpréter correctement la tablette - en se laissant guider par le dessin du carré et de ses diagonales qui accompagne l'image - il convient d'ajouter un *point fractionnaire* : en tête des nombres du haut et du bas ; après l'unité du nombre central. On trouve alors, en base 60 :

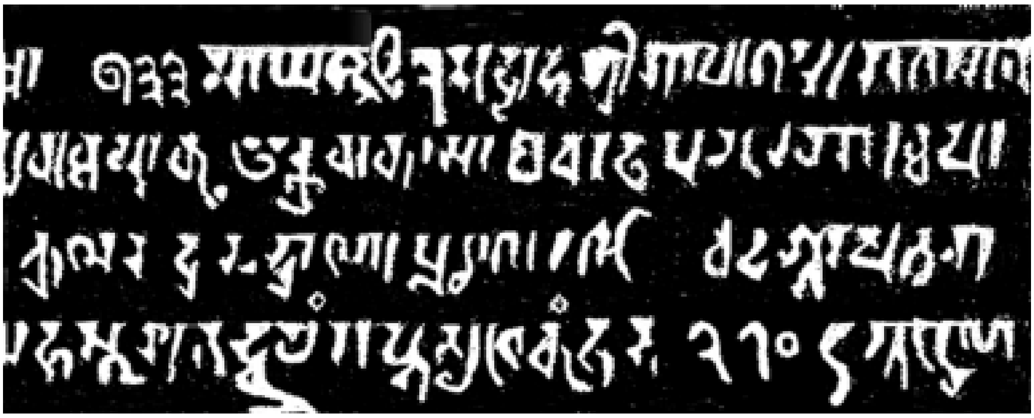
$$[0\cdot 30]_{60} = \frac{30}{60} = 0\cdot 5_{10}$$

$$[1\cdot 24 \quad 51 \quad 10]_{60} = 1 + \frac{24}{60} + \frac{51}{60^2} + \frac{10}{60^3} = 1\cdot 414213\cdots_{10}$$

$$[0\cdot 42 \quad 25 \quad 35]_{60} = \frac{42}{60} + \frac{25}{60^2} + \frac{35}{60^3} = 0\cdot 707106\cdots_{10}$$

Les trois nombres qui figurent sur la tablette babylonienne sont donc un demi 1/2, racine de deux $\sqrt{2}$ et son inverse $1/\sqrt{2}$, en numération sexagésimale.

1.2. Décimal



Ce détail d'une inscription sanskrite contient la plus ancienne écriture attestée de *nombres décimaux*, avec représentation explicite du zéro : 933 sur la première ligne (à gauche) et 270 sur la dernière (à droite). Guitel [1] date son écriture de 876.

Figure III : Stèle de Gwalior.

L'écriture décimale dont la notre dérive naît en Inde au VIII^{e} siècle. Elle représente les nombres entiers avec dix symboles ; y compris le célèbre zéro qui attend ainsi le IX^{e} siècle pour recevoir enfin sa première écriture explicite attestée - fig. III. C'est une acquisition relativement tardive de l'homme.

L'écriture décimale indienne est ensuite adaptée pour la langue arabe. C'est au travers de la civilisation arabe que l'écriture décimale parvient de l'Inde en Occident - voir fig. IV. Il ne s'impose définitivement en Europe que vers le XV^{e} siècle, pour y supplanter la numération romaine.

L’arabe s’écrit de droite à gauche, à l’inverse du sanskrit. Pourtant, l’ordre indien avec le chiffre le plus significatif à gauche est conservé dans l’écriture arabe. Il en résulte que celui qui lit comme celui qui écrit l’arabe doit changer de sens quand il passe du texte aux chiffres. Dans la transcription latine qui suit, les scribes ne prennent pas plus de risques : ils gardent intact l’ordre d’écriture des chiffres arabes. Il en résulte que nous lisons et écrivons les chiffres dans le même ordre que le texte, comme en sanskrit. Le fait que nous sachions lire le fragment en fig. III de la stèle de Gwalior est donc une pure coïncidence : les autres chiffres du document ne sont lisibles que par les érudits. Remarquons enfin que seul le chiffre zéro est resté sans changement ; il s’écrit pareil en sanskrit, arabe et moderne.

Le *système décimal* est devenu aujourd’hui la première partie universelle de l’écriture de l’homme. Au XXI^{e} siècle on écrit les nombres de la même façon du Tibet à la Patagonie, et chacun sait lire et compter les nombres de l’autre, partout dans le monde.

Al Khowarizmi (étymologie du mot algorithme) était un savant persan du IX^{e} siècle. Son ouvrage *Al Jahbar* (étymologie du mot algèbre), regroupe les connaissances mathématiques de l'époque, d'origines grecque, arabe et indienne. C'est un recueil de méthodes de calculs, en particulier les opérations de l’arithmétique décimale, illustré d'exemples significatifs et intéressants.

L'*astrolabe* permet de connaître sa position sur terre, en la comparant à celle des astres vus dans le ciel. Cet instrument sera remplacé d'abord par le *sextant*, puis maintenant par le GPS - *Geographic Positional System*. Le GPS combine trois technologies de pointe - électronique, espace et télécommunication - et il tient aussi dans la main.

Figure IV : Al Khowarizmi tenant l'astrolabe.

1.3. Calculs de romains

La numération romaine est utilisée en Occident jusqu'à la Renaissance et sert encore pour les dates et la pagination. C'est une représentation alphabétique hybride de base 5 où la position d'un symbole faible est soustractive s'il est placé devant le symbole fort, et additive s'il est après. Sa complexité apparaît dans le nombre de règles – taille de l'algorithme - pour convertir un entier naturel *n* en la chaîne de caractères *R(n)* qui représente son écriture en chiffres romains. On écrit l'entier *n* sous forme de suite de chiffres romains en calculant l'expression *R(n)* par application des règles suivantes :

$$\begin{array}{cccll}
1000 \le n < 6000: & R(n) & = & M & R(n-1000) \\
900 \le n < 1000: & R(n) & = & CM & R(n-900) \\
500 \le n < 900: & R(n) & = & D & R(n-500) \\
400 \le n < 500: & R(n) & = & CD & R(n-400) \\
100 \le n < 400: & R(n) & = & C & R(n-100) \\
90 \le n < 100: & R(n) & = & XC & R(n-90) \\
50 \le n < 90: & R(n) & = & L & R(n-50) \\
40 \le n < 50: & R(n) & = & XL & R(n-40) \\
10 \le n < 40: & R(n) & = & X & R(n-10) \\
9 \le n < 10: & R(n) & = & IX & R(n-9) \\
5 \le n < 9: & R(n) & = & V & R(n-5) \\
4 = n: & R(n) & = & IV & R(n-4) \\
1 \le n < 4: & R(n) & = & I & R(n-1) \\
0 = n & R(n) & = & &
\end{array}$$

L'algorithme d'écriture en chiffres romains est présenté ici par des règles de calcul, à utiliser pour remplacer l'expression de gauche par celle de droite quand la condition sur l'argument *n* est satisfaite. Ainsi l'écriture de la date décimale 1997 prend 6 applications des règles :

$$\begin{array}{l}
R(1997) \Rightarrow X \quad R(997) \Rightarrow XCM \quad R(97) \Rightarrow XCMXC \quad R(7) \\
\Rightarrow XCMXCV \quad R(2) \Rightarrow XCMXCVI \quad R(1) \Rightarrow XCMXCVII
\end{array}$$

Songez au problème pratique de calcul posé par cette écriture ! On se fera une idée précise de la difficulté en réalisant le *comput ecclésiastique* de l'an 800 avec les moyens de l'époque. Ceux-ci comprennent les chiffres romains et l'algorithme du calendrier Julien ; l'utilisation d'un abaque auxiliaire est autorisée, mais pas la notation moderne des classes de congruences (modulo), que l'on doit à Gauss.

Bien entendu, il n'est pas demandé de transcrire à chaque étape les résultats intermédiaires pour les écrire en chiffres romains. Ils sont juste gardés sur abaque. La transcription finale et écriture en chiffres romains ne se font donc qu'une fois par résultat final. Nous allons voir – fig. VI - que tous les calculs intermédiaires se passent de fait en décimal, près de mille ans avant la stèle de Gwallior – fig. III.

2. Compter sur les doigts

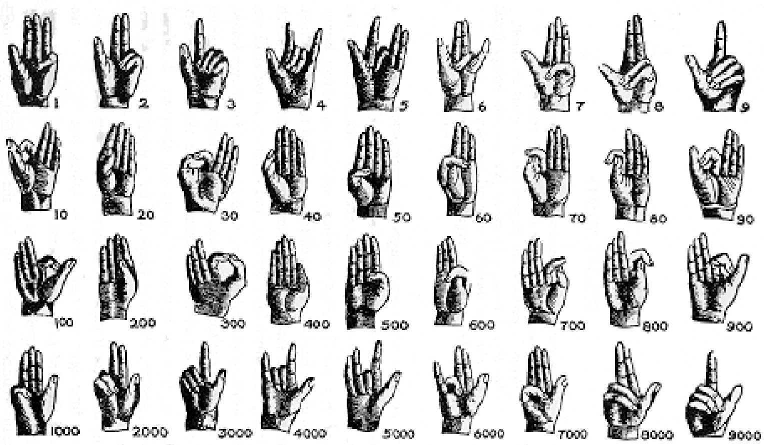


Figure V : Numération sur une main - XIV^{e}.

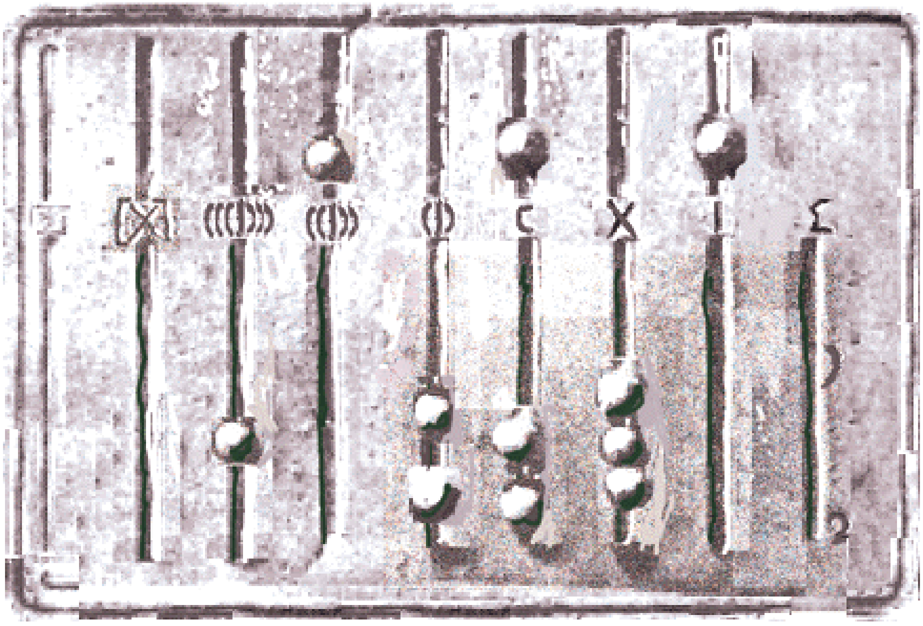
Lucy - notre ancêtre de mille siècles - avait dix doigts. Elle s'en servait pour *compter*, comme vous et moi. Elle lève un doigt par unité de compte. Quand elle arrive à dix, elle retient cette dizaine en levant un doigt de pied. Lucy a un peu d'arthrite ; elle préfère aussi depuis longtemps garder les dizaines dans sa tête, la gymnastique intellectuelle est moins douloureuse. Elle lui permet aussi de s'inventer une nouvelle paire de membres virtuels, sur les dix doigts desquels Lucy compte ses centaines. Elle a la bosse du commerce, et ne se trompe pas à son désavantage. Elle a donc beaucoup d'enfants.

Lucette - fille de Lucy - a l'habitude de compter sur les doigts de sa main gauche ; pour garder la droite libre. Quand elle arrive à cinq, elle ferme la gauche ; elle retient sur un doigt disponible en main droite.
Lucien, son cousin amoureux, compte les dizaines de Lucette. Il a sa propre méthode pour compter. Il garde les deux mains libres pour parler ; les yeux sont presque toujours fixés sur Lucette ; il garde en permanence un pied par terre ou deux. Il retient en marquant les dizaines du doigt sur le sol, avec son autre pied ; il sait aligner soigneusement ses dizaines sur la même colonne. Quand Lucien compte cinq marques alignées, il les efface et les remplace par une marque horizontale, qui vaut cinquante dans cette colonne. Quand deux marques horizontales apparaissent, c'est un jour faste pour Lucette. Lucien doit alors créer une nouvelle colonne, pour les compter les centaines - voire une autre pour les milliers. Il est prêt à tout ; Lucien a inventé le calcul décimal, tel que nous le pratiquons tous !

Cette fable illustre notre conviction que la pratique du compte décimal sur quelques chiffres est beaucoup plus ancienne que tout document, même préhistorique. Ce n'est qu'une opinion : il n'y a aucun espoir archéologique ni d'infirmer, ni de confirmer. Notre croyance vient de l'informatique. Des résultats de complexité montrent que le compte par position – l'algorithme de Lucien – est *optimal*, au choix de la base près – voir [3]. Pour les ordinateurs la meilleure base est 2 ou l'une de ses puissances. Pour les descendants de Lucy qui calculent avec leurs doigts, la base 10 s'impose. Notons que le *compte décimal* de Lucien subsiste de nos jours, en dépit de multiples tentatives de le remplacer par d'autres systèmes ; tous se sont révélées moins ergonomiques. Voir fig. V pour apprendre à faire des erreurs !

Regardons ce qui se passe dans la période historique qui suit, soient 4000 ans. Il est intéressant ici de contraster les représentations utilisées pour écrire les nombres - sur la pierre, le papyrus, la terre cuite - de celles qui servent à les coder sur abaque de calcul.

2.1. Abaque de calcul



Cet abaque romain est un boulier décimal. Les chiffres sont marqués par des cailloux. Le nom latin pour caillou est *calculus* - étymologie du mot calcul. Les lettres au centre indiquent la valeur des cailloux placés en bas de colonne ; un caillou placé en haut de colonne vaut cinq fois plus. Sauf pour celle de droite qui contient des nombres fractionnaires, chaque colonne correspond à une puissance de dix, de 1 à 10 millions. L'image ci-dessus représente donc l'entier décimal 152 735.

Figure VI : Abaque romain.

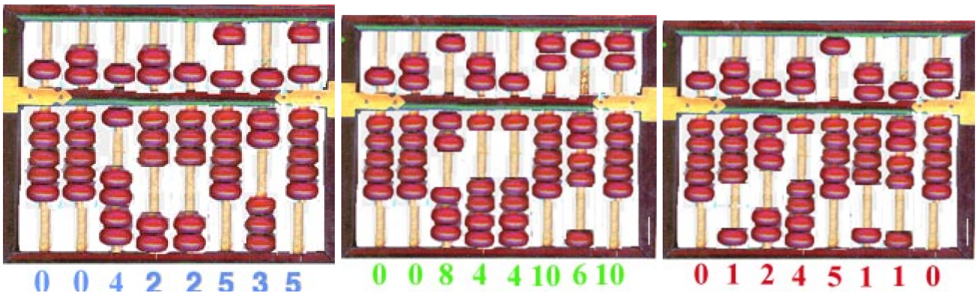
Dès l'aube de la civilisation, l'homme append à mener des calculs plus complexes en déplaçant des cailloux sur un abaque de sable, de pierre ou de bois. Le boulier - fig. VII - est la forme contemporaine de cet outil ancestral - fig. VI - encore largement utilisé dans le monde. Un compromis aussi harmonieux entre ergonomie, simplicité et coût reste encore aujourd'hui hors de portée de la concurrence électronique, dans bien des cas pratiques.

En contraste avec la grande variété des écritures des nombres de l'homme, les représentations des nombres sur les abaques de calcul utilisent presque uniformément - et depuis la plus haute antiquité - le système décimal et ses variantes simples. L'histoire des calculs sur abaques - qui est moins bien documentée - semble donc beaucoup plus simple que celle des numérations écrites. Presque tous les instruments dont nous ayons gardé trace reposent sur le système décimal de position - au codage des chiffres, et au support près - sable, bois, pierre, papier. Zéro se marque invariablement, et très économiquement, par une colonne vide.

Ainsi les Romains - dont nous avons montré que la numération écrite est particulièrement complexe - utilisaient les mêmes abaques – fig. VI - que les Grecs (dont la numération écrite n'était guère meilleure) et que les Egyptiens, les Chinois, les Indiens et les autres. L'utilisation du système décimal dans les calculs pratiques précède - à en croire notre fable initiale - son écriture explicite de plusieurs millénaires. Les Indiens n'ont pas découvert le zéro ; ils lui ont juste donné une écriture simple, qui est devenue *norme universelle* dans les langages de l'homme.

2.2. Calcul sur boulier

Notons en passant que, sur leurs abaques, les Babyloniens devaient prendre soin de reporter les retenues à 6 sur les colonnes paires, et à 10 sur les impaires - fig. VII. Les Babyloniens avaient des abaques semblables à celles des Egyptiens et des Romains, mais ils s'en servaient de façon différente - machines identiques, autres algorithmes - base 10 dans un cas, base 60 codé en décimal dans l'autre.



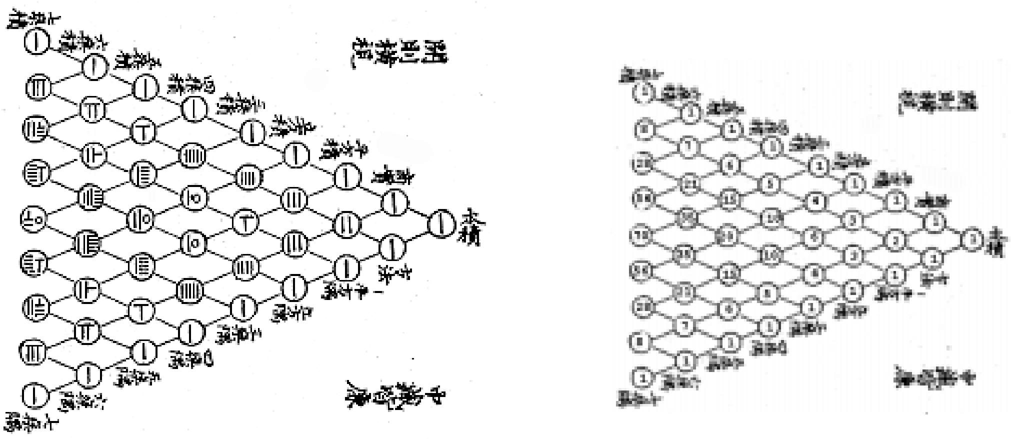
Configuration initiale. On double chaque colonne. On passe les retenues.

On vérifie, par un calcul en base 60 sur le boulier, qu'on a bien $2B=H$ où $B=(42+(25+35/60)/60)/60$ et $H=1+(42+(25+35/60)/60)/60$ sont les deux nombres de la tablette de Yale – fig. II.

Figure VII : Calcul sexagésimal, sur boulier chinois.

2.3. Notation du boulier

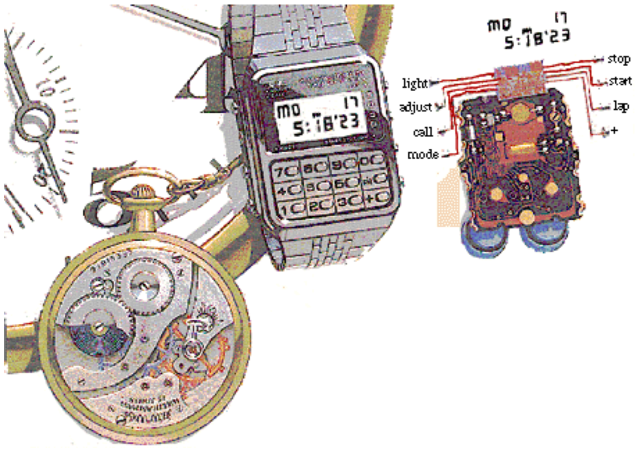
L'adoption du système décimal permet de transcrire sur le papier les résultats des calculs du boulier, et de les conserver pour référence. Ceci ouvre la porte à des calculs plus longs et plus fiables. L'algèbre permet alors de spécifier l'algorithme par une suite d'expressions qui économise les opérations à calculer pour le jeu d'entrées.



Le triangle de Pascal, tel qu'il se présente (après rotation d'un quart de tour) sur la couverture d'un livre chinois de 1303 - d'après Guitel [1]. Les chiffres bâtons sont une transcription, dans l'écriture du Chinois, les configurations du boulier sur lequel ils déplaçaient des bâtonnets de bambou. Le zéro – qui figure explicitement quatre fois – sert à marquer sans ambiguïté les colonnes vides.

Figure VIII : Triangle de Pascal en chiffres bâtons.

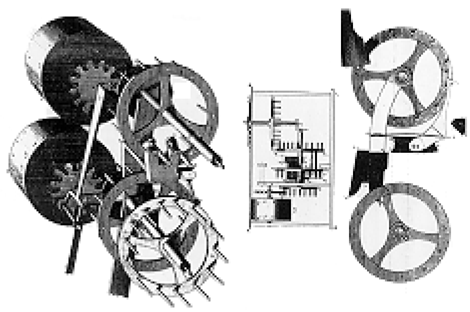
2.4. Calcul mécanique



Le report alterné des retenues à six et à dix – voir fig. VII - est précisément ce que fait toute montre mécanique ou numérique quand passe chaque seconde. L'algorithme de décompte du temps, que nous avons gardé des Babyloniens, reste donc indépendant de sa technologie de réalisation - de la terre cuite au silicium, en passant par bien d'autres formes d'abaques de calcul.

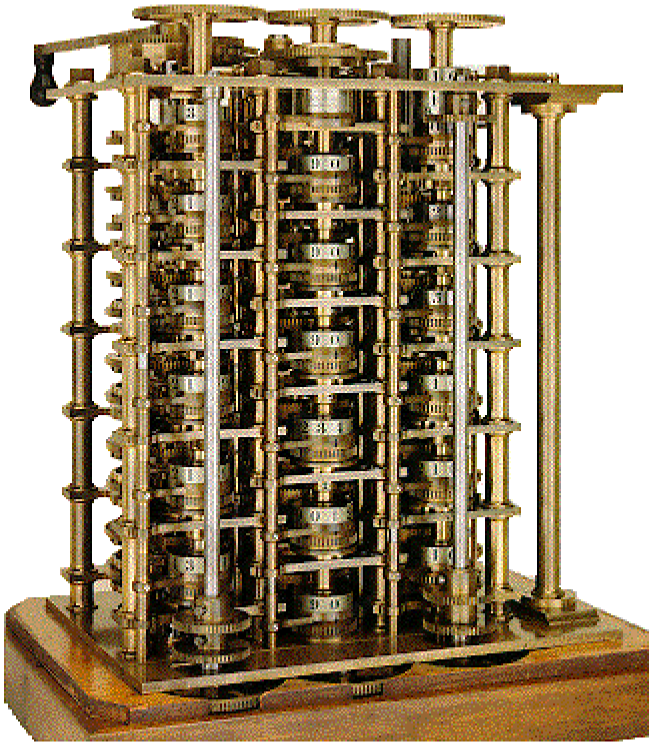
Figure IX : Montres.

Avec les algorithmes, les applications du calcul se multiplient au fil des âges. Il faut calculer le calendrier, les impôts, les récoltes, les plans, les marées, les cartes, les trajectoires et bien d'autres choses. L'homme qui calcule les opérations de ces algorithmes devient une forme de *machine universelle,* capable de les réaliser tous. Ainsi, les marins, les astronomes, les banquiers et les savants du XVI^{e} siècle faisaient tous leurs calculs à la main, en s'aidant de tables numériques propres aux algorithmes de chaque métier. Les limites de cette méthode ne concernent pas la nature des calculs - ils sont en théorie arbitrairement complexes ; elle vient de leur longueur. Même si certains opérateurs humains réussissent à calculer un chiffre d'addition décimale par seconde dans la durée, la fatigue amène forcement des erreurs à la longue. Comme les tables dont ils se servent sont-elles aussi calculées à la main avant d'être reproduites, elles contiennent souvent des erreurs. Tous les calculs manuels deviennent donc faux au-delà d'une certaine longueur - qui dépend bien sûr du soin de l'opérateur. Les meilleurs mathématiciens - qui savent pourtant vérifier leurs calculs et éliminer les fautes - en ont tous fait, des petites comme des grosses.



Extrait de l'Encyclopédie de Diderot, rubrique arithmétique et calcul.

Figure X : Report des retenues dans la machine de Pascal.



Cette partie de la machine différentielle de Babbage est assemblée en 1832 par Clement. Elle comprend plus de 2 000 engrenages, et a coûté £ 20 000 à l'amirauté britannique. Elle marche toujours impeccablement - mais ce n'est qu'une partie du plan initial.

Figure XI : Machine différentielle de Babbage.

C'est pour tenter de réduire les erreurs et donc de permettre des calculs plus longs que les savants et les ingénieurs réalisent des machines mécaniques, à commencer par la *Pascaline* en 1642 – fig. X. Il s'agit de reproduire mécaniquement l'algorithme d'addition décimale avec report des retenues – celui de Lucien !

Ces mécaniques issues de l'horlogerie culminent en 1832 avec la réalisation de la machine différentielle de Babbage – fig. XI. C'est une machine spécialisée dans l'évaluation de polynômes de degré 6 aux valeurs entières consécutives. Sa fonction est de calculer automatiquement et sans erreur les tables dont se sert l'amirauté britannique. Il marche encore mais son développement n'a pas suivi. Il suffit en effet d'un tour de manivelle pour voir s'afficher l'entrée suivante de la table. Mais il reste encore à reporter à la main et sur du papier les chiffres lus aux cadrans de la machine. C'est long et des erreurs s'introduisent quand même. Au-delà des succès techniques et scientifiques bien reconnus, toutes ces machines sont des échecs économiques. Elles sont trop chères, trop fragiles et trop lentes pour remplacer de façon rentable le papier et le crayon alliés à l'intelligence humaine. Ces calculateurs mécaniques à engrenages ne seront véritablement utilisés dans le commerce comme caisses enregistreuses que pendant la première moitié du XX^{e} siècle.

2.5. Calcul d’image

Dans le métier à tisser, le motif à réaliser est codé sur des cartes perforées qui commandent directement la mécanique servant à lever les trames. Suivant qu'une trame est levée ou non, le fil attaché à la navette passe au-dessus ou au-dessous du point correspondant qui devient visible ou non dans l'image tissée au final.

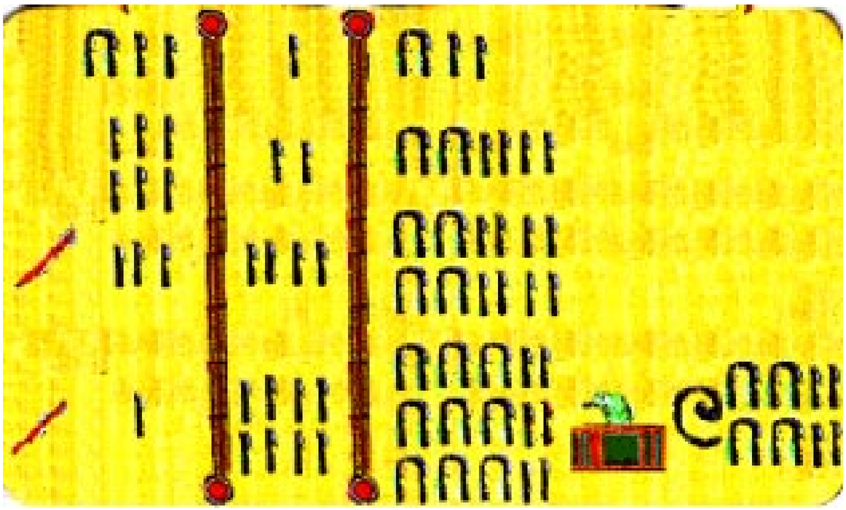
Figure XII : Métier à tisser Jacquard.

Près d'un siècle après la machine à additionner de Pascal, Jacquard invente un dispositif à aiguilles et cartons perforés qui permet de contrôler automatiquement (numériser, programmer) les motifs à réaliser par le métier à tisser – fig. XII. En 1801 le *métier Jacquard* - muni de 24 000 cartes - tisse le portrait de son concepteur. Cette machine spécialisée dans la reproduction sur la soie d'images numériques connaît un grand succès - Lyon compte plus de 30 000 métiers Jacquards à la mort de son inventeur en 1834. Avec la mécanisation vient aussi la révolte sociale des *canuts* ; pour chaque machine introduite un emploi est supprimé - Jacquard fut sauvé plusieurs fois par la police de tentatives contre sa vie.

Plus calme socialement est le disque rigide à ergots qui remplace le carton perforé dans les automates issus de l'horlogerie helvétique. Pour la bonne vitesse de rotation, on fait jouer de la musique numérique par des marionnettes animées et des pianos mécaniques - premier multimédia digital en temps réel ?

En combinant un lecteur de cartes perforées à un compteur mécanique, Hollerith gagne le contrat des machines de recensement aux Etats Unis ; il fonde une compagnie en 1896 dont le nom deviendra *IBM* - International Business Machines - en 1924.

2.6. Multiplication Egyptienne : du papyrus au silicium



D'après le papyrus de Rhind, vers -1700. Malgré son âge vénérable l'algorithme de multiplication décrit ci-dessus est très actuel. Il est utilisé systématiquement dans tous les microprocesseurs dont l'unité arithmétique et logique ne permet que le calcul direct d'additions et de décalages.

Figure XIII : Multiplication binaire, sur papyrus.

La vitesse de calcul des opérations sur les bouliers stagne pendant plusieurs millénaires et les seuls progrès significatifs viennent des *algorithmes*, c'est à dire des méthodes de calcul utilisées. L'histoire de ce sujet est aussi riche qu'ancienne. Ainsi, l'algorithme de multiplication binaire par additions et décalages se pratique sur tous les microprocesseurs, inchangé depuis plus de 4000 ans - fig. XIII.

En généralisant à partir de l'exemple donné, le papyrus de Rhind - fig. VII - nous dit que le produit $n \times m + p$ se calcule $M(n, m, p) = n \times m + p$ par les règles suivantes :

$$\begin{aligned} &M(0, m, p) \Rightarrow p \\ &M(2n, m, p) \Rightarrow M(n, 2m, p) \\ &M(1+2n, m, p) \Rightarrow M(n, 2m, p+m) \end{aligned}$$

Vérifions le déroulement de cet algorithme de multiplication égyptienne dans le calcul du produit de douze par douze :

$$\begin{aligned} 12 \times 12 &\Rightarrow M(12, \quad 12, \quad 0) \\ &\Rightarrow M(6, \quad 24, \quad 0) \\ &\Rightarrow M(3, \quad 48, \quad 0) \\ &\Rightarrow M(1, \quad 96, \quad 48) \\ &\Rightarrow M(0, \quad 192, \quad 144) \Rightarrow 144 \end{aligned}$$

On retrouve la transcription décimale des trois colonnes du papyrus de Rhind. A gauche de la première colonne, on trouve la représentation binaire de $n = 12 = 8 + 4 = 1100$ - verticale, poids faibles en haut ; pas de marque pour un bit nul, une marque diagonale pour les bits impairs. La dernière ligne du calcul, pour n=0, est reportée en bas à droite : c'est le produit final 144.

3. Système binaire

Figure XIV : Décomposition numérique de l'œil d'Horus, d'après K. Sethe.

L'usage du système binaire est fécond au travers des mathématiques antiques – fig. XIII et XIV. Il faut cependant attendre 1703 pour que Leibnitz montre explicitement la profonde simplicité des quatre opérations arithmétiques – addition, soustraction, multiplication, division - dans cette numération. Entré dans la pratique mathématique depuis lors, le système binaire se marie enfin aux techniques électroniques - relais, lampes à vide, et surtout transistor - pour devenir le codage de choix des nombres dans les machines du XX^{e} siècle. Regardons pourquoi et comment le système binaire est devenu, en cinquante ans, un langage indispensable aux communications de l'homme.

3.1. Pourquoi ?

Fiabilité Mesurer une variable physique, c'est la classer parmi un nombre fini d'états discernables – on dit que l'on numérise cette mesure. La précision de cette numérisation est limitée par les erreurs de mesure – on modélise par un bruit aléatoire qui vient s'ajouter au signal à mesurer. Le choix qui minimise l'erreur de mesure est de classer la variable parmi deux états – le 0 et 1. Ainsi, la probabilité d'erreur d'une porte logique élémentaire dans un circuit électronique moderne est largement inférieure à 10^{-20}. Sinon, un calcul d'une heure sur un microprocesseur - environ 10^{20} opérations binaires par heure - ne réussirait quasiment jamais à finir sans faute.

Dans un circuit intégré, la distance de communication est de l'ordre du *micromètre* – $1\mu = 10^{-6}$m – le rapport *signal/bruit* très grand. Dans les images transmises par les sondes planétaires, c'est l'inverse ; la distance de communication se mesure en millions de km, et le signal est infinitésimal en regard du bruit cosmique. Pourtant, c'est ici encore le système binaire qui s'impose, grâce aux *codes correcteurs* qui nous viennent des mathématiques et de l'informatique. Ce sont des algorithmes qui permettent de particulariser et de faire durer le signal émis, assez pour permettre au récepteur de retrouver le message d'origine, petit à petit dans le bruit détecté.

Simplicité et coût Les quatre opérations +, -, x, / de l'arithmétique entière sont calculs les plus utiles, que l'on retrouve au travers de toute application. Il est donc crucial que le dispositif qui va réaliser ces calculs soit aussi simple, et donc petit et fiable que possible. Prenons pour exemple la multiplication, puisque le papyrus de Rhind – fig. IX – nous en a déjà livré le secret binaire.

Quand on explique le système binaire aux enfants, ils ne l'aiment pas car il y a plus de chiffres. En échange, la table de multiplication binaire n'a que 4 éléments, contre 100 en décimal. Une analyse montre que le *rendement par bit* de la multiplication décimale est 69% de celui de la multiplication binaire. Par la même mesure, le rendement de la base 60 est 96%. Pour l'addition, on trouve un rendement binaire 120% meilleur que le décimal, et que tout autre base – sauf les puissances de 2, qui ont même rendement que le binaire. Voir [3] à ce sujet.

Pour cette raison, les multiplicateurs que l'on réalise sur silicium sont tous en base 2 – multiplication égyptienne. Ils sont plus petits que ceux des autres bases - dans le rapport donné par le rendement ci-dessus. Quand on multiplie ce gain par des millions de circuits, on comprend que les lois de l'*économie* viennent à ce point promouvoir aussi le système binaire.

Universalité En 1936, la *thèse* de Church et Turing caractérise mathématiquement ce qui est *calculable automatiquement*, et ce qui ne l'est *pas*. Turing propose une machine *universelle* capable à elle seule d'effectuer *tout* calcul qui est réalisable automatiquement, par un moyen physique quelconque, à la taille et à la vitesse près. Ceci vaut modulo un codage des données d'entrée et de sortie du calcul au travers du système binaire.

Dans son célèbre papier de 1947 intitulé *Mathematical Theory of Communication*, Claude Shannon explique comment la transmission de toute forme d'information peut se décomposer en *suite binaire,* et pourquoi cette décomposition est adaptée à la réalisation de système de télécommunication optimal.

Depuis, ces théories sont mises en pratique quotidienne avec les réseaux d'ordinateurs. Le système binaire permet de représenter toute information - texte, image, son, … - aux fins de transmission, stockage et traitement. . Le microprocesseur est une machine capable de faire tous les traitements.

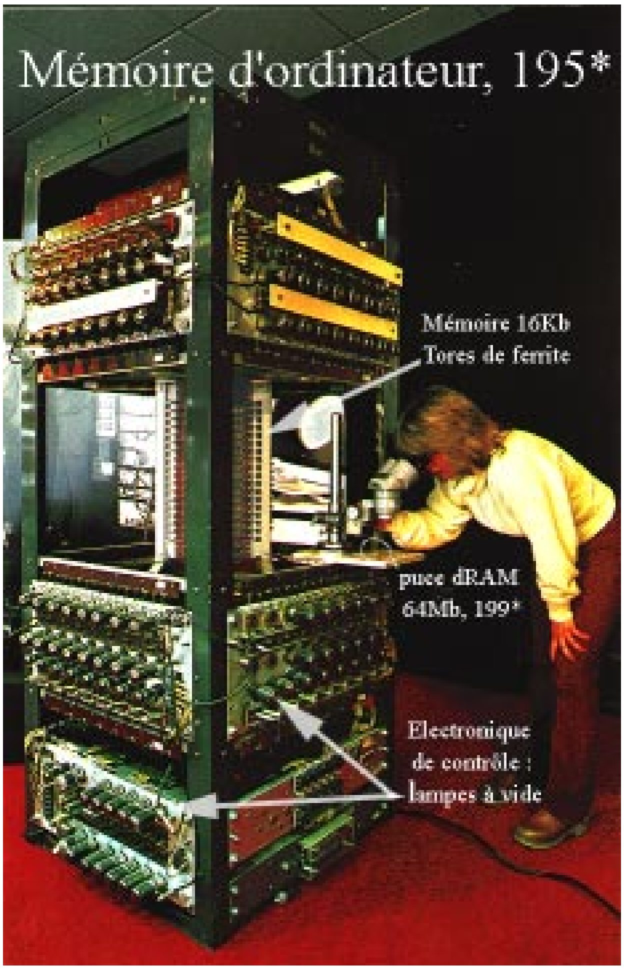


Figure XV : Mémoire d'ordinateur, avant le transistor.

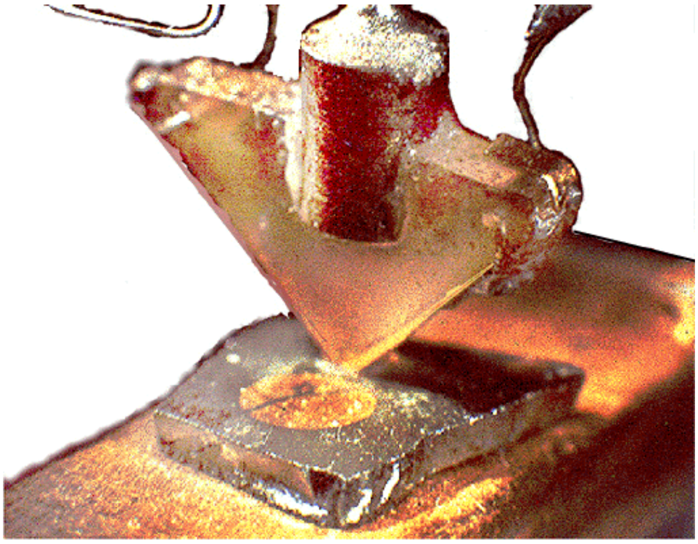


Figure XVI : Le premier transistor, Bell Laboratories 1947.

3.2. Comment ?

Jusqu'à la dernière guerre mondiale, les questions de calcul ne sont primordiales ni dans les sciences, ni dans les techniques. Le système binaire reste d'usage confidentiel. Les besoins en calculs militaires - radar, sonar, cryptographie, bombe atomique, calculs balistiques, … - vont changer la situation.

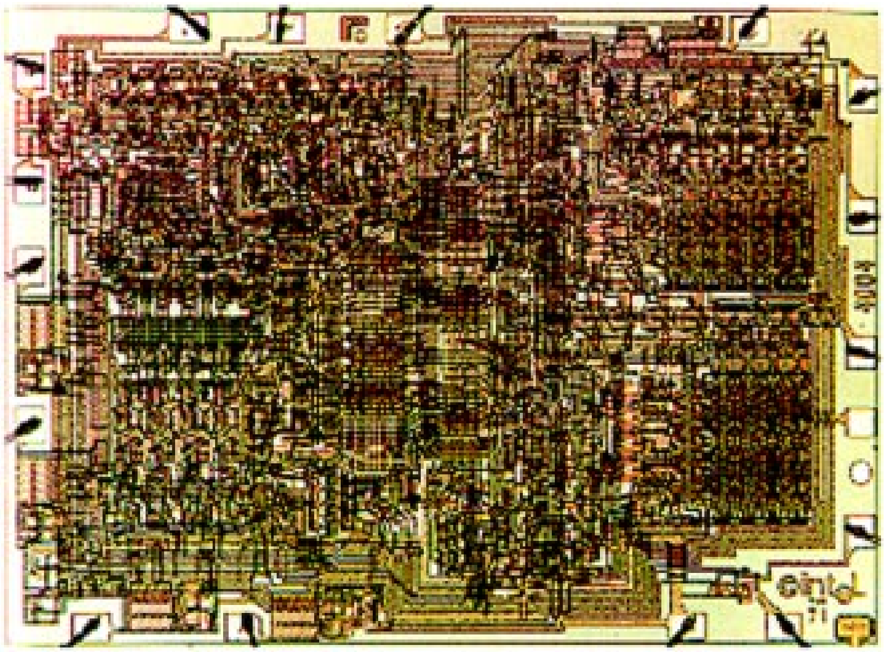
C'est à partir de 1947 - année de naissance du transistor, de l'ordinateur programmable et de la théorie mathématique de la communication - que s'amorce un phénomène de *boule de neige* entre science, technologie et économie, qui fait basculer le monde dans un nouvel *Age*, celui de l'information.

4. Histoires digitales

Dans les années 50, la radio à transistors, économique et portable, offre au monde la communication de masse par les ondes. Les bénéfices en retour servent à financer la mise au point de la technologie suivante. C'est le circuit intégré des années 60 – fig. XVII. On *intègre* de plus en plus de transistors connectés sur le même support physique à état solide. En combinant tous ces transistors sur une seule *puce*, on peut réaliser des fonctions de plus en plus complexes, comme par exemple celles de la calculatrice électronique. Fin 60, elle remplace la règle à calcul dans les lycées, et rentre dans l'électronique *grand public*. Dans le même temps, la radio bénéficie aussi des circuits intégrés ; elle étend son marché, par des modèles de haute fidélité, comme par des modèles miniature à portée de toutes les bourses de la planète.

Il en va de même pour l'ordinateur qui avance à grand pas de *puce*, avec la gamme *360* d'*IBM* ; cette société devient alors l'une des premières compagnies mondiales, et elle domine l'informatique pour plus de vingt ans. La grande nouveauté de ces systèmes est de permettre l'exécution des logiciels sur toutes les machines de la gamme. Ceci permet aux clients de conserver et d'accumuler leurs propres applications, au travers des fréquents changements de matériels auxquels ils vont finir par s'habituer.

Pour répondre aux besoins de ses clients - fabricants japonais de calculatrices, *Intel* développe en 1971 le *I4004*, premier microprocesseur 4 bits – fig. XVII. Il intègre sur une même *puce* les trois composantes d'une machine *universelle* : unité de calcul, mémoire des données et mémoire des instructions. Cette combinaison unique de composants remplace par autant de programmes les opérateurs câblés qui se multiplient alors pour les calculettes : addition, soustraction, multiplication, division, racine, exposant, logarithme, …



Ce processeur 4 bits I4004 de la compagnie *Intel* contient 2 300 transistors. Gros comme un ongle de bébé, il coûte $200 en 1971. Il calcule plus vite que les premiers ordinateurs, mille fois plus chers.

Figure XVII : Le premier microprocesseur, 1971.

C'est dans la conquête de l'espace, le contrôle des machines à laver, et d'autres applications tout aussi inattendues que le microprocesseur, cet outil à tout faire, connaît ses premiers succès industriels. Deux ans après son introduction, le microprocesseur connaît plus de 2000 applications, dont aucune n'avait été prévue par ses concepteurs. Il faut pourtant attendre 1979 pour que le microprocesseur commence à trouver aussi sa place actuelle, au cœur de la structure des ordinateurs.

4.1. Loi de Moore

La multiplication des applications augmente d'autant les volumes de production des circuits intégrés ; ceci permet de diminuer les coûts unitaires, et de financer les investissements nécessaires pour réduire encore la taille des composants. Les avantages techniques et économiques de cette *miniaturisation* sont alors clairs. En 1973, G. Moore - président et cofondateur d'*Intel* - prédit que le nombre de transistors par puce va doubler tous les dix huit mois. Cette prédiction, connue sous le nom de *Moore's law*, s'est révélée correcte depuis près de trente ans. En devenant plus petit, le circuit intégré gagne en vitesse, en fiabilité, et il devient moins cher. Ceci permet de baisser continuellement les coûts des applications existantes. Chaque gain de puissance lui ouvre la porte de nouvelles applications. Chaque baisse dans le coût des calculs élimine des techniques concurrentes, qu'elles soient mécaniques ou humaines.

Un autre développement majeur des années 70 est rendu possible par la combinaison du circuit intégré et des télécommunications numériques : le commutateur téléphonique *automatique*. C'est un progrès technique important : d'objet de frustration perpétuelle (Allo ! le 22 à Asnière ?), le téléphone devient soudain fiable, et beaucoup plus utile.

Ce progrès a aussi des conséquences sociales majeures : le métier d'*opérateur téléphonique* disparaît. Des centaines de milliers de gens, surtout des femmes à l'époque, doivent changer d'emploi. C'est la première fois que l'informatique déplace aussi brutalement un métier. Ce n'est pas la dernière. Les emplois peu qualifiés sont remplacés par une solution automatique dès que celle-ci devient économiquement compétitive. En échange, on crée des emplois plus qualifiés, dans la conception, la programmation, la fabrication, la vente et la maintenance de ces solutions, à base de calcul automatique.

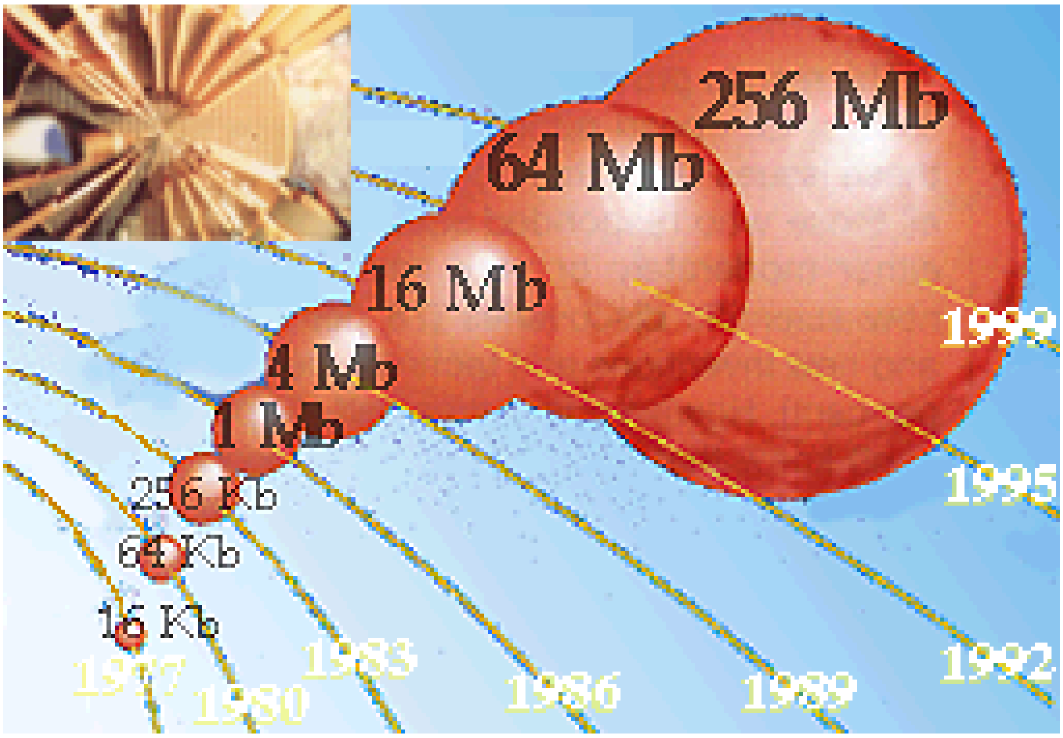


Figure XVIII : Evolution des mémoires dRAM.

Souvent, ces nouveaux métiers de l'informatique sont eux aussi éphémères : on a vu les perforateurs de cartes, les pupitreurs, les opérateurs d'ordinateurs, les techniciens de maintenance, … Ces métiers ont disparu aussi vite qu'ils sont venus. Leurs titulaires ont dû acquérir de nouvelles qualifications : expert en traitement de texte, programmeur, ingénieur système, maintenance par réseaux … Les programmeurs COBOL ont dû apprendre le langage C++, et maintenant JAVA.

4.2. Naissance d'une industrie

Dans les années 80, le mini-ordinateur VAX de *Digital* rend le calcul accessible à une multitude de chercheurs, enseignants, ingénieurs, gestionnaires, dans tous les métiers de l'homme. Ceci prépare la multiplication - qui va suivre - des applications de l'informatique à chacune de nos professions : de l'avocat au biologiste et au livreur de pizza.

Les *réseaux d'ordinateurs* arrivent à maturité durant la même décennie. Ils permettent depuis lors de réserver un vol d'avion - en temps réel - partout sur le globe. Ils permettent aussi de contrôler des chaînes d'assemblage automatiques, dans lesquelles des robots travaillent. Les humains, ici encore, sont déplacés par la machine : des emplois de basse qualification disparaissent ; d'autres, plus qualifiés mais moins nombreux, apparaissent.

Dans le même temps, le microprocesseur couplé à la mémoire RAM – fig. XVII - devient l'outil de base de toute l'informatique *embarquée* : dans les avions, les autos, les satellites, les missiles, les bateaux, les robots, les sondes spatiales, les téléphones, …

La part de l'informatique dans le coût d'une voiture haut de gamme monte régulièrement ; pour approcher aujourd'hui le quart ! Fin 70, on prédisait que l'automobile fournirait vite le premier marché de l'électronique ; il se vendait alors bien plus de voitures que de microprocesseurs. Il est vrai maintenant que toute voiture neuve comporte plusieurs processeurs, voire une dizaine. C'est un marché substantiel ; il est moins important que celui des millions de processeurs que l'on vend chaque jour sur les cartes à puces et chaque mois dans les PC.

Le pilote d'un avion moderne - *fly by wire* - conduit avant tout un ordinateur complexe, qui est maintenant seul aux commandes *directes* des ailerons, des moteurs, de la radio, météo et de la navigation.

L'argent électronique stocké en binaire par des charges magnétiques dans les ordinateurs du monde entier a une somme bien supérieure à tout ce qu'on garde dans les porte-monnaie et dans tous les coffres-forts ; pour un volume bien moindre. La valeur des échanges journaliers d'argent électronique *virtuel* est pour plus de dix fois celle des réserves des banques centrales de tous les états de la planète.

En devenant digital, le téléphone revient aux principes de son ancêtre, le télégraphe. Et le son prend une autre dimension. Il devient aussi image et texte. On le transmet, d'ordinateur en ordinateur à une vitesse proche de celle de la lumière. La communication, à toute distance et sous toutes formes, est devenue affaire informatique, avant tout. Ou l'inverse, si vous préférez. Pourtant, il n'est plus de réseau sans ordinateur, plus d'ordinateur sans réseau.

L'imprimerie, par laquelle Gutenberg a changé le monde, est désormais numérique. Il y a cinquante ans, la page que vous lisez aurait demandé plusieurs tonnes d'équipements, et des centaines d'heures de travail avant de pouvoir être imprimée sur papier. Elle a été composée sur un PC -*Personal Computer* - portable de moins de cinq kilogrammes, en quelques heures. Elle est imprimée sur une imprimante de bureau en couleur qui revient - en 1997 - moins cher à l'année d'usage que le téléphone - achat, papier et encre compris. Par la magie des réseaux numériques - au travers d'une puce MODEM de 1 cm^2 - je peux tout aussi bien la faire imprimer - en quelques minutes - depuis chez moi comme en Australie.

C'est pour toutes ces raisons que les technologies de l'information sont devenues la toute première industrie de l'homme, en moins de cinquante ans.

> *The overall electronics industry represents the United States' largest manufacturing business (1989 revenue: $ 300 billion), bigger than steel, aerospace and automobile combined.*
>
> Time magazine, Dec. 4, 1989.

5. Langages de l'Internet

Vers la fin des années 70, le département américain de la défense installe le réseau *Arpanet* pour permettre la communication numérique – courrier électronique, transfert de fichiers - entre ses centres de recherche, divers industriels, les universités et d'autres. Une spécification du cahier des charges n'est pas ordinaire : en cas destruction d'une partie du réseau – lire bombe atomique à cette époque de guerre froide – la partie survivante doit rester à même de communiquer. L'architecture résultante est nécessairement *distribuée* : bien que sa finalité ultime soit militaire, il n'y a aucune forme de *coordination centralisée* dans ce réseau.

La contrainte est que toute tentative de communication peut *échouer*, sans conséquence dramatique pour les autres. Ce n'est pas le cas dans les réseaux téléphoniques ; on se souvient de quelques coupures fameuses du téléphone, à l'échelle de tout un pays pendant des heures, suite à une *bogue* dans quelque programme - le système de comptabilité du réseau ou ailleurs. Par son architecture *Internet* permet de fusionner, localement et sans difficulté technique, tout réseau indépendant à l'ensemble, et donc de croître en agrégeant des bouts disparates. Dans les années 80, ce sont les Universités et centres de recherche du monde entier qui viennent se greffer, et contribuer en échange au développement de cet outil de communication qui leur devient vite indispensable.

Les compagnies multinationales se dotent alors aussi, les unes après les autres, d'un réseau de communication interne - *Intranet* – conçu sur les mêmes principes que *l'Internet*, mais juste utilisé à l'intérieur de l'entreprise. Des ponts entre réseaux publics et réseaux privés s'établissent, au travers des *Firewall*. L'entreprise trouve alors assez d'intérêt à l'usage libre du réseau externe pour y contribuer, en échange gratuit, les cycles inutilisés sur son réseau de communication interne. Ceci multiplie d'autant, pour tous et localement, la bande passante disponible pour le *club* des utilisateurs de *l'Internet*. C'est ainsi que le nombre de serveurs Internet passe de 213 en 1981 à 160 000 en 1990.

Ceci épuise la majorité des membres institutionnels d'*Internet* : compagnie, organisme d'état, université et centre de recherche majeur, au travers du monde.

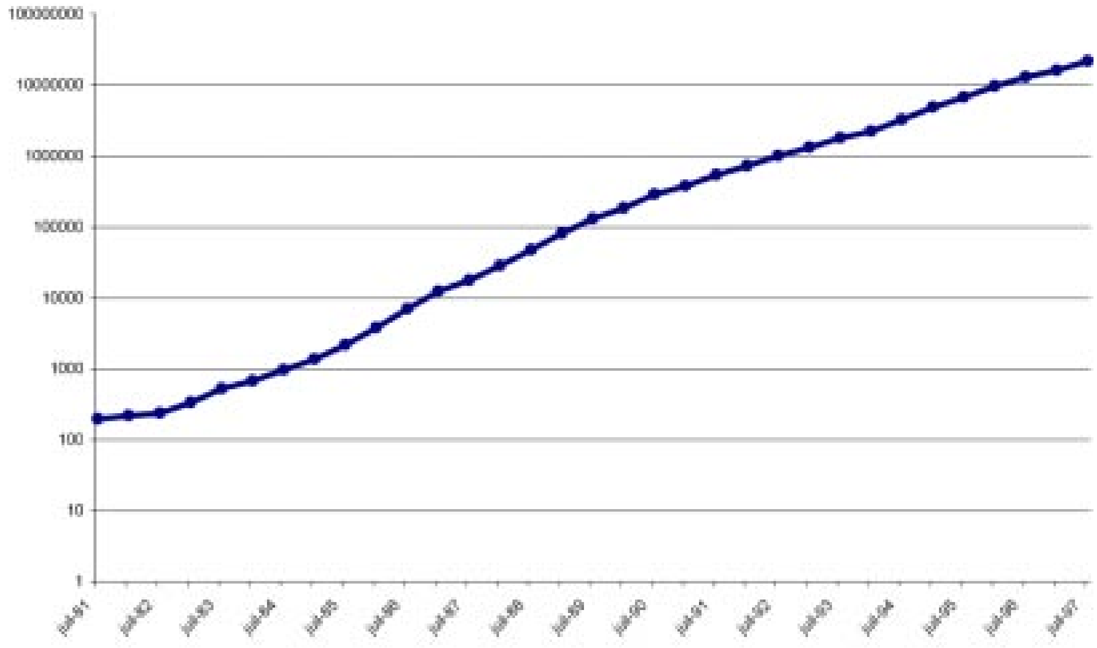


Figure XIX : Croissance du nombre des *Internet Hosts*.

La phase de croissance de l'*Internet* qui suit est tout aussi spectaculaire, même par les critères blasés de l'informatique en ces domaines. Les physiciens du CERN ont besoin d'un langage commun pour échanger les informations scientifiques dans les groupes internationaux liés à l'activité des grands accélérateurs. Le résultat est HTML – *Hyper Text Markup Language* – qui permet l'échange de documents scientifiques : textes et bientôt images fixes. Ce nouveau langage numérique ne semble pas révolutionnaire au premier abord. La syntaxe de HTML –codage numérique des phrases du langage - est inutilement complexe, voire ambiguë me disent certains collègues. Même avec les systèmes de visualisation – *browser* – et d'édition les plus modernes, la composition et la publication de pages HTML reste une activité bien complexe, au goût de beaucoup. La lecture des documents est beaucoup plus simple. Toujours est-il que HTML devient un succès instantané dans les Universités, puis auprès du grand public vers le début des années 90.

C'est le *Minitel rose* qui donne à l'époque l'impulsion initiale, et transforme cette technologie audacieuse en succès commercial hexagonal. La transmission d'images pornographiques joue plus tard le même rôle catalyseur, et contribue à déplacer l'*Internet* hors du bureau, dans les cafés et à la maison. Les physiciens qui ont mis au point HTML n'avaient pas prévu cet usage de leur langage : ils visaient juste à permettre de transmettre les images de collision dans les accélérateurs.

Heureusement, de multiples applications plus avouables et socialement utiles suivent de près, sur le *Minitel* comme sur l'*Internet*. Les *médias* en parlent tous les jours. La croissance phénoménale du nombre d'utilisateurs alliée aux possibilités techniques d'Internet ouvre la porte à bien des fantasmes virtuels – bibliothèque et encyclopédie universelle, Tour de Babel, etc.

Beaucoup métiers de basse qualification vont maintenant disparaître au profit de réseaux de machines. La banque de demain sera accessible 24h/24 de tout point de l'Internet, et offrira des services nouveaux. De nouveaux métiers - de plus haute qualification - vont aussi résulter de cette nouvelle mutation technologique. La banque de demain aura moins de guichets humains, et on en attendra beaucoup plus qu'aujourd'hui. On peut prévoir une mutation comparable dans l'agence de voyage, les petites annonces, la vente aux enchères, la grande distribution, la publicité, l'information, les divertissements, et bien d'autres services.

Aujourd’hui, HTML est devenu le seul langage numérique compris, lu et écrit dans le monde entier. Il est aussi interprétable par toutes les marques et tous les systèmes d’ordinateurs. C’est le premier langage informatique à avoir attend ce statut de *standard mondial*. On peut inclure des images, du son et tout ce que les ordinateurs savent représenter et manipuler. Le texte sur *Internet* se trouve dans toutes les langues de la planète.
On peut ajouter que l’Internet apporte aussi sa contribution à faire du *bad english* la langue de communication universelle. Ceci nous amènerait à parler des langages pour l’homme, un tout autre sujet ; restons en à notre propos, les langages pour les machines.

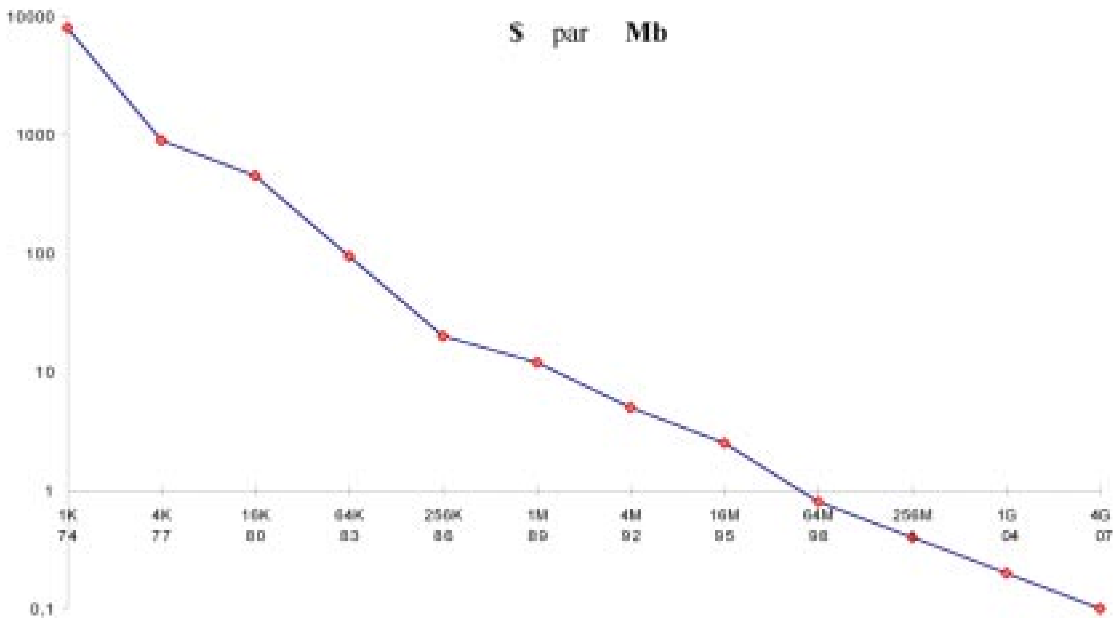


Figure XX : Evolution du prix de la mémoire ***dRAM***.

5.1. Aujourd'hui

L'âge de l'Information souffle vigoureusement ses cinquante bougies ; il va croître et embellir pendant de nombreuses années encore. Tout devient numérique. Tout devient connecté. Les applications se multiplient. Les technologies convergent. Ce que la *forme* du calcul gagne - taille, vitesse, coût - sa *fonction* le récupère en généralité et (quelques fois) en simplicité d'usage.

Avec la convergence actuelle de la radio, de la télévision, du cinéma de la photographie et des télécommunications vers le *tout digital*, on sait déjà comment utiliser les cycles du PC de l'an 2003, seize fois plus puissant que celui d'aujourd'hui, à en croire la loi de Moore. Le vidéophone, la reconnaissance de la parole - donc commande vocale - et la télévision numérique haute définition sur grand écran deviennent alors possibles en temps réel.

Après avoir informatisé ses machines, l'homme semble parti pour informatiser ses propres *services*. Le couplage d'un réseau de communication mondial avec une puissance de calcul à coût infinitésimal ouvre des possibilités techniques fantastiques. Dans les braves nouveaux mondes digitaux que l'on imagine alors, l'informatique semble ici encore devoir déplacer de multiples métiers dans les services ; ce sont d’ailleurs en partie ceux qui avaient remplacé les métiers de l'industrie, disparus lors de la dernière informatisation des machines de production : textile, automobile et autres.

Demain ?

Combien de temps la spirale informatique va-t-elle encore tourner à cette vitesse ?

La loi de Moore deviendra forcement fausse ; c'est le lot de tout phénomène naturel dont la croissance initiale semble exponentielle. Pourtant, elle est exacte depuis plus de 30 ans, pendant lesquels la densité de calcul du silicium s'est multipliée par plus de 1000. Parions ici que la loi de Moore va s'appliquer pendant au moins trois générations technologiques, soit encore plus de 10 ans. C'est en tous cas ce que prédisent les tables de l'industrie des semi-conducteurs, dont l'objectif est 0.1 μm en 2007.

Ce sont les lois de l'économie avant celles de la technologie qui actionnent et régulent la *loi de Moore*. Une usine de silicium *state of the art* coûtait déjà plus d'un milliard de $ en 1995, et le prix double aujourd'hui avec chaque génération de technologie. Pendant combien de temps la croissance du marché justifiera de la rentabilité d'investissement aussi colossaux, avant que le phénomène ne ralentisse ?

Quand le nombre d'électrons utilisés pour stocker le 1 logique descend de quelques milliers à quelques centaines, les lois de la mécanique statistique cèdent progressivement le pas à celles de la mécanique quantique. Les lois de l'électronique changent à cette échelle. Par exemple, il n'y a plus de gain en vitesse d'horloge en retour de la miniaturisation. Ces phénomènes nous attendent aux alentours de 0.05 μm. Dans 15/20 ans, à en croire Moore ? On trouvera des références sur les limites physiques intrinsèques aux calculs MOS dans [4].

Nous n'avons parlé ici que de technologies et d'applications qui sont bien connues aujourd'hui. Il y a gros à parier que nos *machines à tout faire* trouveront des applications nouvelles, aussi importantes économiquement que celles que l'informatique a su dénicher par le passé et que personne n'avait prévu. De plus, le calcul optique, quantique, biologique ou autres pourrait devenir un jour plus rentable que le calcul sur silicium, et contribuer ainsi à amplifier le progrès technologique global.

6. Références

[1] G. Guitel, *Histoire comparée des numérations écrites*, Flammarion, Paris, 1975.

[2] O. Negeubauer, *The Exact Sciences in Antiquity*, Princeton University Press, 1952.

[3] D. E. Knuth, *The Art of Computer Programming*, Volume 2: *Seminumerical Algorithms*, Addison-Wesley, 1980.

[4] M. V. Wilkes, *The cMOS end-point and related topics in computing*, in *IEEE Trans. Computers*, Computing & Control Engineering Journal, pp.101--106, I.E.E. 1986.

[5] C. Houzel, *L'invention du zéro*, *Pour La Science*, No 228, pp.12--15, octobre 1996.