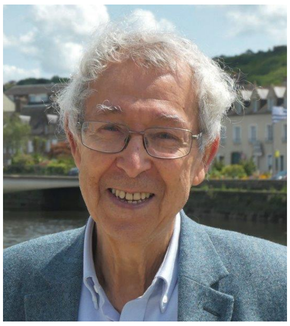
La saga des nombres.

Du zéro à l'infini :
La grande saga des nombres



Ahmed Djebbar,

Historien des sciences.

Sommaire

Le zéro existait dans différentes traditions scientifiques antérieures à la civilisation de l'islam. Mais c'est celui de la tradition indienne qui a circulé à partir du VIIIe siècle, d'abord à Bagdad. Les mathématiciens de Bagdad ont découvert la puissance du zéro, qui simplifiait les calculs. Les Grecs ont inventé la démonstration. Les Arabes ont compris qu'il fallait se servir des apports grecs et indiens.

Pour en savoir plus, il faut citer quelques ouvrages : « *L'Afrique compte !* » de Claudia Zaslavsky, « *Histoire universelle des chiffres* » de Georges Ifrah, ou « *Histoire d'algorithmes*[1] » de Jean-Luc Chabert.

I. Au commencement :

Bois de renne
30.000 av. J.C.

L'os d'Ishango
23.000 ans av. J.C.

Au début, il n'y avait pas d'historiens des mathématiques. Des chercheurs ont construit un scénario qui semble vrai.

On a dû commencer par observer l'environnement, écouter, nommer des éléments en se servant du développement des langues ; toutes ces pratiques étaient liées aux besoins des utilisateurs.

Mémoriser, compter, marquer…

Les plus anciens indices retrouvés sont des bois de renne, découverts en Europe et datant de 30.000 av. J.C., contenant des séries de points et d'encoches

[1] Algorithme : technique de calcul.

Plus tard, vers 23 000 ans av. J. C., l'os d'Ishango (découvert en Afrique) est recouvert de traits…

On ne sait pas ce que signifiaient ces points et ces encoches.

Calculer, c'est utiliser le comptage, imaginer des opérations pour obtenir le résultat cherché.

On pense donc que le calcul est arrivé avant l'écriture, dans le croissant fertile, en Mésopotamie.

I. Les premiers pas :

Les anciens connaissaient le soleil, la lune. D'où, et avant l'arrivée des religions, l'idée de l'unité.

Puis est arrivé l'idée de la dualité. Dans certains peuples, le duel est plus important que l'unité.

D'autres peuples sont passés, directement, du singulier au pluriel. Beaucoup de langues ont utilisé ou utilisent encore le duel, comme le breton, l'arabe classique, le gallois, l'hébreu, le macédonien etc.

Pour certains peuples, le pluriel commence à partir de trois.

Ensuite il y a les ensembles nombreux, ceux que l'on maîtrise ou pas, jusqu'à ceux qu'on ne peut classer, comme l'infini.

Comment considérer les grands nombres qu'on ne peut pas compter facilement ? On les regroupe par paquets.

On a compté par paquets de 2 : d'où la base 2

On a aussi utilisé d'autres bases :

5, 10, 20 (pour les calculs habituels)

24, pour parler du nombre d'heures dans la journée

60, pour optimiser les opérations sur les fractions de 60 qui deviennent des entiers, en particulier pour faire des opérations sur les minutes et les secondes.

Comment considérer la multitude, comme le nombre de poissons dans un banc de poissons, le nombre de grains de sel dans la salière ?

Dans ce cas, on ne peut constituer des bases ; on va alors se servir d'autres outils.

On va peser, puis comparer, mesurer le volume de deux substances et comparer.

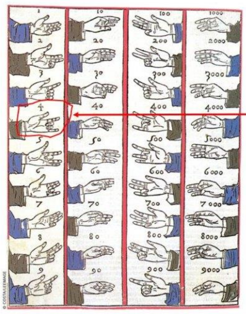
Donc, au lieu de compter, on compare.

Plus grand que la multitude, il y a l'innombrable, l'infiniment grand comme le nombre d'étoiles. On parle ici d'infini, c'est-à-dire ce que l'on ne peut pas compter.

On dira qu'un ensemble d'éléments est infini lorsqu'on peut toujours ajouter 1 à un nombre donné d'éléments de cet ensemble.

Au XIX^{ème} siècle, on considèrera que l'infini est un concept spécial que l'on peut manipuler comme un nombre.

I. Les débuts de la numérisation :



Numération digitale

Il faut créer des outils pour gérer les nombres de la vie courante.

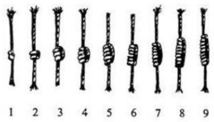
On imagine associer un groupe d'éléments à un autre, quand c'est possible.

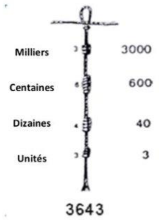
On choisit un objet référent, plutôt petit et pratique, comme un gland.

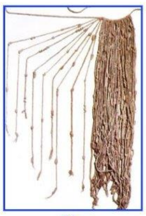
On associe 1 mouton à 100 glands, une pomme à 10 glands.

Ou on se sert d'une partie du corps, nos doigts par exemple, qui selon qu'ils sont pliés ou dépliés, représenteront des nombres.

On peut associer un nombre d'objet à des cailloux, à des ficelles,







Qipu

La Guinée avait créé une monnaie locale, appelée « cauri » du nom d'un coquillage bien connu dans le pays.

Des peuples d'Amérique latine utilisaient des cordes tressées, les quipus, pour leurs opérations.

Peu à peu, on va inventer des outils de calculs.

On va calculer en base 10, 60…

La base 5 (numération quinaire) était également utilisée en Afrique, en Amérique latine, au Cambodge….

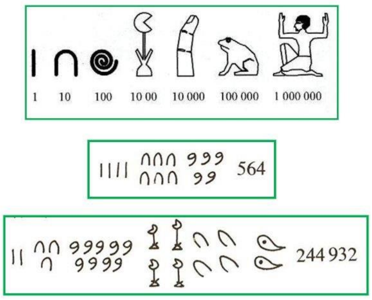
0 → 0
1 → 1
2 → 10
3 → 2 & 1 = 10 & 1 = 11
4 = 2x2 = 10x10 = 100
5 = 101
6 = 110
7 = 111

D'autres peuples d'Afrique Amérique du sud, Océanie ont utilisé la base 2

C'est cette base qui est utilisée en informatique. En informatique, l'énergie est fournie par l'électricité, laquelle ne connaît que deux états : le courant est coupé (état 0) ou il passe (état 1).

Cela peut paraître long de calculer en base 2, mais les ordinateurs savent travailler très vite.

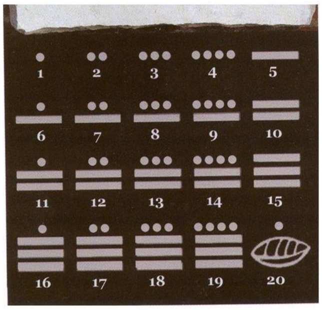
A. Numération egyptienne :



Elle prend de la place, mais reste toujours lisible, quelle que soit la manière de représenter un nombre dans l'espace. Elle ne connaît pas le zéro, ni comme élément représentant l'absence de chiffre, ni comme nombre.

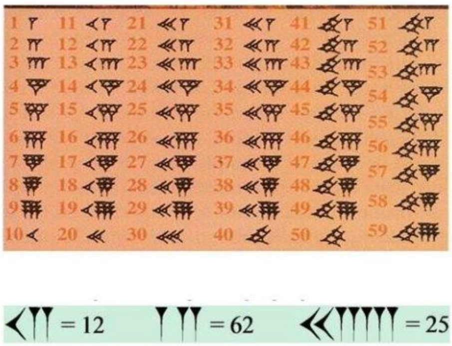
Elle est relativement sophistiquée.

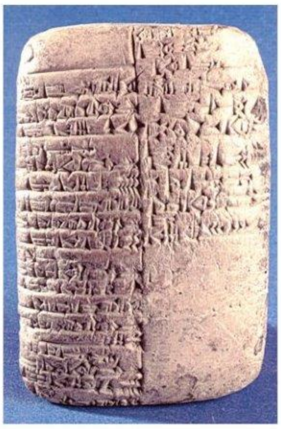
A. Numération maya :



Le nombre 20 est représenté par un cauri.

B. Numération babylonienne :





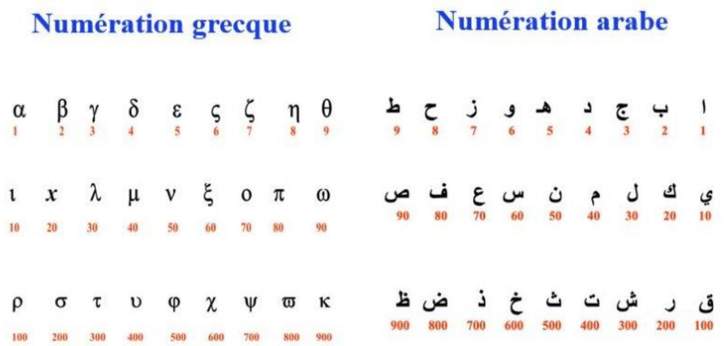
Écriture cunéiforme, sophistiquée, mais ne comportant toujours pas de zéro.

Des objets archéologiques relatifs à cette numération auraient été volés lors de l'invasion de l'Irak.

Les signes sont des clous ou des chevrons, et utilisent la base 60.

Un clou vaut 1 ou 60 ou 60^2 ou 60^3. Le contexte est donc indispensable pour connaître la valeur d'un nombre.

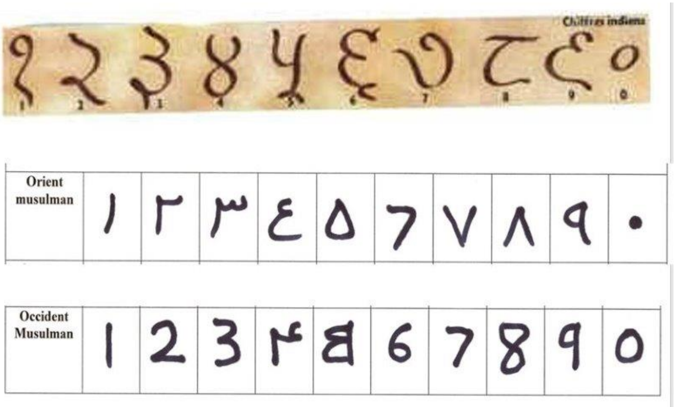
C. Numération alphabétique :



Ces systèmes ont duré longtemps.

Puis arrive la numération indienne.

A. Numération indienne :



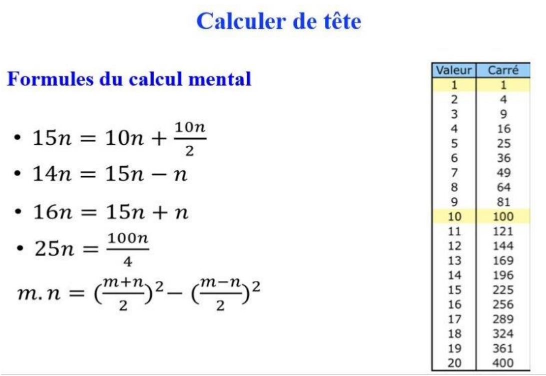
Cadeau scientifique : le zéro fait son apparition. Les mathématiciens à Bagdad ont probablement joué un rôle dans la modification de la graphie de certains des neuf chiffres.

On pense qu'à la longue, le 0 s'est transformé en point.

L'occident musulman l'a utilisé à partir du X^{ème} siècle, et il s'est ensuite répandu en Europe.

I. Différents procédés de calcul :

Différentes techniques ont peu à peu vu le jour.

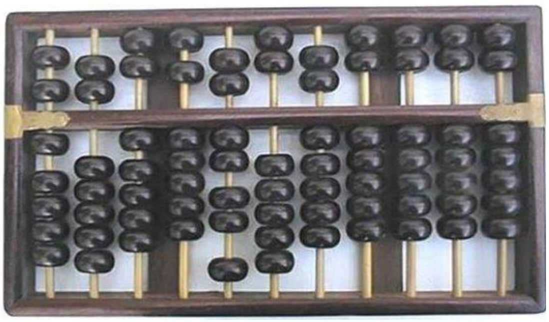


Le calcul mental :

Il ne s'agit pas d'essayer de refaire mentalement ce que l'on pourrait faire avec un crayon, mais d'adapter les opérations au calcul oral.

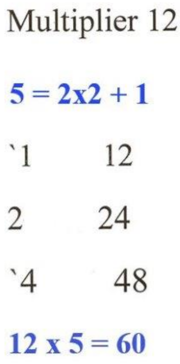
Exemple : pour multiplier un nombre quelconque, *n*, par 15, il suffit de le multiplier par 10, puis d'en calculer la moitié. On ajoute ensuite les deux nombres trouvés et on obtient le résultat.

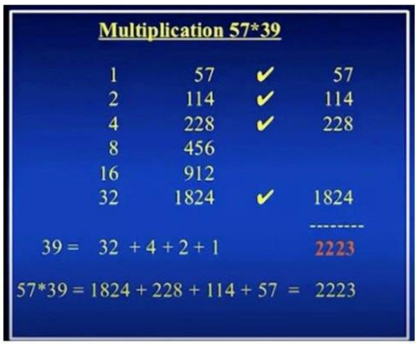
Le boulier chinois :

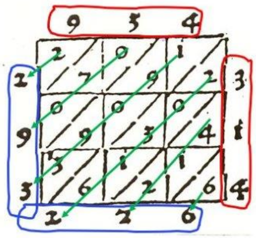


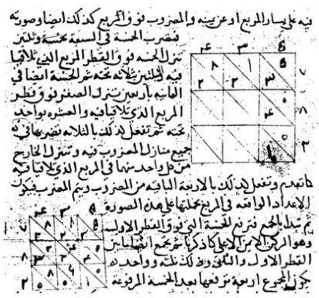
Les bouliers chinois sont en base alternée (5, 2) pour lesquels chaque tige comprend deux parties : une partie supérieure sur laquelle les boules valent 5 unités (ou 5 dizaines, 5 centaines… selon la position de la tige) et une partie inférieure sur laquelle les boules valent 1 unité (ou 1 dizaine, 1 centaine… selon la position de la tige).

Calculer comme les scribes égyptiens :



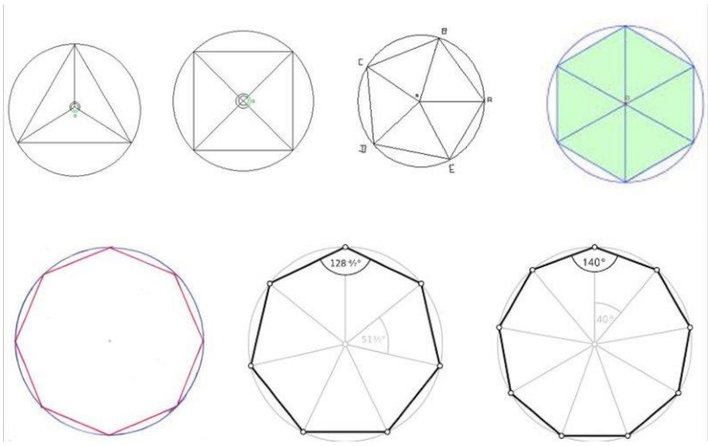






Ou avec la technique du grillage :

I. Les nombres en géométrie :



On peut chercher à inscrire un
On peut chercher à inscrire un polygone dans un cercle. Un triangle ou un carré s'inscrivent facilement avec un compas. Mais lorsque le nombre de côtés augmentent, il arrive un moment où ce n'est plus possible avec ces méthodes simples.

Pour cela, il faudra recourir à d'autres techniques.

I. Extension des nombres :

On a bientôt eu besoin d'étendre la notion de nombre.

On a ainsi inventé :

es fractions, les nombres irrationnels[2], les nombres réels positifs (tout rapport de grandeurs incommensurables : racines cubiques, rapport du périmètre d'un cercle à son diamètre (π), etc…), les nombres négatifs, les nombres réels quelconques (l'ensemble des nombres rationnels et irrationnels), les nombres imaginaires : i *tel que :* $i^2 = -1$, inventé par un mathématicien de Bologne. On s'en sert en

[2] Un nombre irrationnel ne peut s'écrire sous forme de fraction.

cours de calcul, puis ils finissent par disparaître, à la fin de la procédure. Ils permettent de déterminer les solutions positives d'une équation du troisième degré.

Revenons aux nombres entiers
Les nombres sont infinis, qu'ils soient pairs, impairs, premiers[3], etc…
Peut-on concevoir plusieurs infinis ? Existe-t-il une relation d'ordre entre les infinis ?
Oui répondaient certains théologiens du moyen âge.

Dans la tradition scientifique grecque, les mathématiciens ont cherché à trouver les nombres premiers d'une suite de nombres entiers donnés (1, 2, 3, 5, 7, ….). C'est ce qu'a fait Ératosthène au II^ème^ siècle. Mersenne (mort en 1648), a cherché à déterminer les nombres premiers qui sont sous la forme : $2^n - 1$ et qui porteront le nom de « *nombres de Mersenne* ». En 1876, Edouard Lucas réussit à déterminer un nombre de Mersenne très grand. En 2009, on en a trouvé un qui s'écrit avec 12.837.064 chiffres. Cela a demandé 29 jours de calcul à l'aide de milliers d'ordinateurs connectés.

Mais à quoi peuvent bien servir de nos jours les nombres premiers ?
Ils servent à sécuriser les données, les transactions, les messages secrets, etc...

Depuis la nuit des temps (chez les Égyptiens, les Romains, etc …) on utilisait une forme de codage des messages secrets que l'on appelle aujourd'hui la cryptographie symétrique. Elle utilise une même clé pour coder et décoder un message.

En 1976, on a inventé la cryptographie asymétrique. Pour décoder un message, elle utilise deux clés, l'une publique et l'autre privée, selon le principe suivant :

Le destinataire du message secret choisit deux très grands nombres premier ***p*** et ***q***.

Il calcule leur produit ***n***.

Puis, avec un algorithme spécial, il calcule deux nombres appelés « *clé de chiffrement* » et « *clé de déchiffrement* ».

Il envoie, à l'expéditeur du message secret, le nombre ***n*** et la clé de chiffrement.

L'expéditeur crypte son message secret à l'aide de la clé de chiffrement et du grand nombre ***n***.

Quand le destinataire reçoit le message chiffré, son ordinateur le décrypte avec la clé de déchiffrement (qu'il est le seul à connaître) et qui utilise les deux nombres premiers ***p*** et ***q*** (qu'il est le seul à connaître).

----

[3] Un nombre premier est un nombre qui n'est divisible que par 1 ou par lui-même.