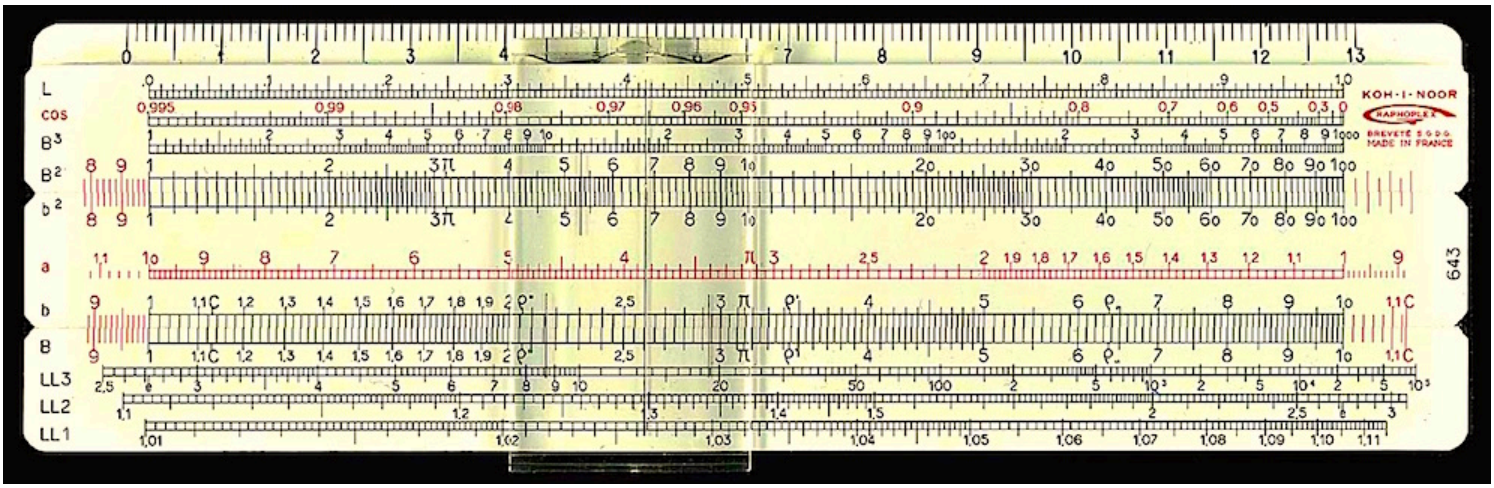
DAILY SCIENCE
DÉCOUVREZ LA SCIENCE, LA RECHERCHE ET L'INNOVATION "MADE IN BELGIUM"

LA MULTIPLICATION : DES CRUES DU NIL À LA CRYPTOGRAPHIE

Publié le 16 mars 2015



PODCAST

Vous disposez d'un passeport, d'une carte de crédit? Il y a fort à parier que ces documents contiennent un peu d'intelligence mathématique développée par le Pr (émérite) Jean-Jacques Quisquater (UCL). Le scientifique, ingénieur civil et docteur en informatique, a mis au point, en 1989, une méthode de cryptage pour les premières « cartes à puce ». Une méthode toujours utilisée actuellement qui s'appuie sur la multiplication et son corollaire, la division. Deux opérations qu'on apprend à l'école dès le plus jeune âge…

« La méthode que j'ai élaborée permet de calculer facilement des divisions et surtout, les restes des divisions », explique-t-il. « On en s'en rend pas toujours compte, mais le reste est en réalité la partie la plus importante de ce type de calculs! »

Une méthode présente dans deux milliards de cartes à puce

En 1989, les premières puces électroniques étaient peu performantes. « Elles ne disposaient que d'une mémoire limitée », se souvient le mathématicien. « Quand on m'a demandé d'implémenter des méthodes cryptographiques pour ces cartes, j'ai repris le problème de la multiplication, de la division et du calcul de reste à zéro. C'est comme cela que la « méthode Quisquater » est née. Améliorée en 1995, elle est aujourd'hui présente dans deux milliards de cartes à puce dans le monde ».

La méthode développée par le scientifique repose sur des opérations arithmétiques de base: la

multiplication, qui n'est qu'une suite d'additions rappelle-t-il volontiers, et la division, avec le calcul du reste.

De Babylone aux tables de logarithmes

L'histoire de la multiplication fascine le chercheur. Il en propose d'ailleurs une relecture, au Collège Belgique. « Il s'agit d'un voyage en deux temps », explique-t-il. « Dans un premier temps, nous plongerons aux origines de la multiplication, qui remonte à Babylone en passant par l'Egypte antique, pour arriver à l'élaboration des tables de logarithmes. Ces tables ont été mises au point pour simplifier les calculs compliqués que posaient les progrès en astronomie. Dans un second temps, nous explorerons la genèse des machines à calculer mécaniques pour aboutir aux cartes à puces ».

Parmi les machines préférées du chercheur, on retrouve la règle à calcul. « Inventée en parallèle aux tables de logarithmes, c'est un engin extraordinaire », s'exclame le chercheur. « Elle est portable, elle est petite, elle est relativement simple à utiliser et est capable de réaliser de nombreuses opérations tout en permettant de stocker, de manière très compacte, de nombreuses tables: tables de logarithmes, table des sinus, tables des cosinus, etc. Pendant plus d'un siècle, la règle à calcul a été l'outil de faveur des ingénieurs.

> ***Deux rendez-vous au Collège Belgique***
>
> *Le Pr Quisquater donnera deux leçons au Collège Belgique, ces 17 et 24 mars 2015, à Bruxelles. La participation à ces leçons intitulées « Multiplions et divisons les nombres: du cadastre des Babyloniens au paiement électronique actuel », est gratuite. La réservation est cependant souhaitée.*