

Enfin, encore en 1905, il publie un autre article intitulé « L'inertie d'un corps dépend-elle de son contenu en énergie ? » qui démontre la fameuse formule d'équivalence masse-énergie $E = mc^2$. Il s'agit d'un résultat de la toute nouvelle **relativité restreinte**, qui sera d'une importance capitale pour un nombre de champs d'études insoupçonnés alors : physique nucléaire, mécanique céleste . . . jusqu'aux armes et centrales nucléaires.

☛ **Stanley Milgram** (New York, 15 août 1933 - New York, 20 décembre 1984) est un psychologue social américain. Il est principalement connu pour l'**expérience de Milgram** (sur la soumission à l'autorité) et l'expérience du petit monde. Il est considéré comme l'un des psychologues les plus importants du XX^e siècle.

De 1960 à 1963, Milgram mène une série d'expériences, avec plusieurs variantes, visant à estimer à quel point un individu peut se plier aux ordres d'une autorité qu'il accepte, mais qui entre en contradiction avec sa conscience. Il demande ainsi à des sujets de donner des chocs électriques à des personnes lorsqu'elles répondent non correctement à des questions. Les personnes qui répondaient aux questions étaient souvent des collègues ou des acteurs destinés à tester les sujets quant à leur obéissance à faire qqchse contre leur conscience. Certaines personnes feignaient des cris, prétextant des douleurs intenses aux chocs électriques, d'autres ont carrément feint la mort.

Les résultats ont montré que les sujets pouvaient ressortir définitivement traumatisés de cette expérience. En 1962, l'*American Psychological Association* suspend son adhésion à cause de questions concernant l'**éthique de ces expériences**. Les résultats surprenants et assez inquiétants, mais aussi la méthode, ont provoqué de nombreux remous au sein de la communauté des psychologues et de l'opinion publique.

En 1967, Milgram reprend une idée développée en 1929 par Frigyes Karinthy : la **théorie des six degrés de séparation**. Milgram essaie de démontrer que tout être humain peut assez facilement être relié à un autre par une chaîne de relations sociales : il s'agit de l'expérience du petit monde.

Et pour l'histoire de **l'informatique** en particulier . . .

☛ L'histoire des nombres

☛ Les bases

Les nombres sont apparus il y a très longtemps, aux environs de 30 000 av. J.-C. L'être humain eut très tôt la nécessité de compter et de dénombrer diverses choses (bêtes, personnes ou objets). Ainsi, comme tout le monde a commencé à compter sur ses doigts, la plupart des civilisations adoptèrent un **système de numération en base 10**. Quelques civilisations choisirent la **base 12**. Les Mayas, Aztèques, Celtes et Basques, comptant aussi avec les orteils, adoptèrent la **base 20**.

☛ Les premiers systèmes de numération

Des entailles faites sur des os d'animaux ou sur les parois de cavernes préhistoriques à côté de dessins d'animaux ne laissent aucun doute sur la fonction de comptabilité.

Un système plus récent (8 000 av. J.-C.) a joué un rôle important dans l'histoire des chiffres : le tas de cailloux. Cette méthode est à l'origine des **bouliers chinois**, encore en usage de nos jours. Ainsi le mot **calcul** vient du latin *calculus*, signifiant « petit caillou ».

☛ Les chiffres

c'est vers 3600 av. J.-C. qu'apparurent **les chiffres**, symboles graphiques pour représenter des quantités numériques. La Fig. 4 montre que les populations du bassin méditerranéen avaient des systèmes de numération très proches.

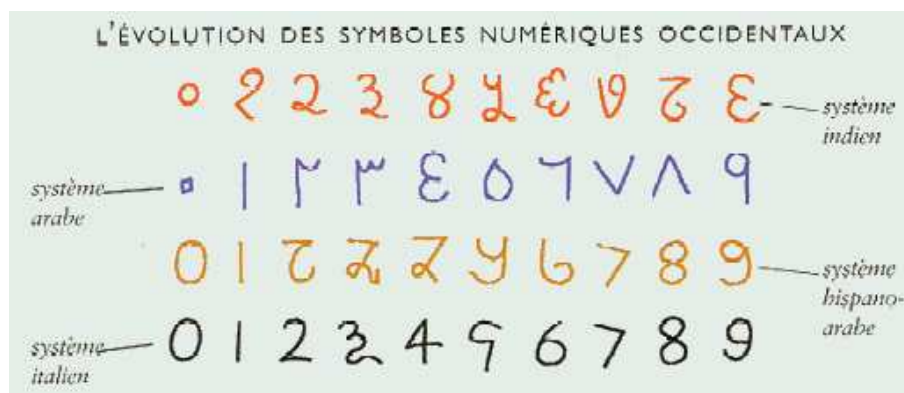


FIGURE 4 – Évolution des symboles numériques occidentaux.

☛ Les nombres

Deux principes permettent de symboliser les nombres : l'un, que l'on peut qualifier de **cardinal**, consiste à adopter un « symbole-étalon » comme représentant l'unité et à répéter ce dernier autant de fois que le nombre considéré contient d'unités ; l'autre, que l'on peut qualifier d'**ordinal**, consiste à attribuer à chaque nombre un symbole original, et donc à envisager une succession de symboles n'ayant aucun rapport les uns avec les autres.

Enfin, pour pouvoir représenter n'importe quelle quantité numérique, la solution a été de privilégier un groupement particulier (dizaine, douzaine, vingtaine ou soixantaine, par exemple) et d'organiser une suite régulière des nombres selon une classification fondée sur ce groupement originel. Autrement dit, on a convenu d'une « échelle » à partir de laquelle il est possible de répartir les nombres et leurs divers symboles suivant des paliers successifs, auxquels on peut donner les noms respectifs d'unités du premier ordre, d'unités du deuxième ordre, d'unités du troisième ordre, etc. De cette façon l'être humain est parvenu à une symbolisation structurée des nombres, permettant d'éviter des efforts de mémoire considérables.

Ainsi un nombre entier quelconque N peut être considéré comme la valeur numérique d'un polynôme $P(x)$ à coefficients entiers positifs, inférieurs à x , x entier positif : x est la **base** de la numération.

$$P(x) = a_m x_m + a_{m-1} x_{m-1} + \dots + a_{m-p} x_{m-p} + \dots + a_0$$

En numération de position, le nombre N est symboliquement représenté sous la forme :

$$a_m a_{m-1} \dots a_{m-p} \dots a_0$$

Prenons l'exemple du nombre 1437. La Fig. 5 montre les représentations analytiques de 1437 où la valeur numérique des coefficients est portée en abscisse et le rang de chaque coefficient en ordonnée.

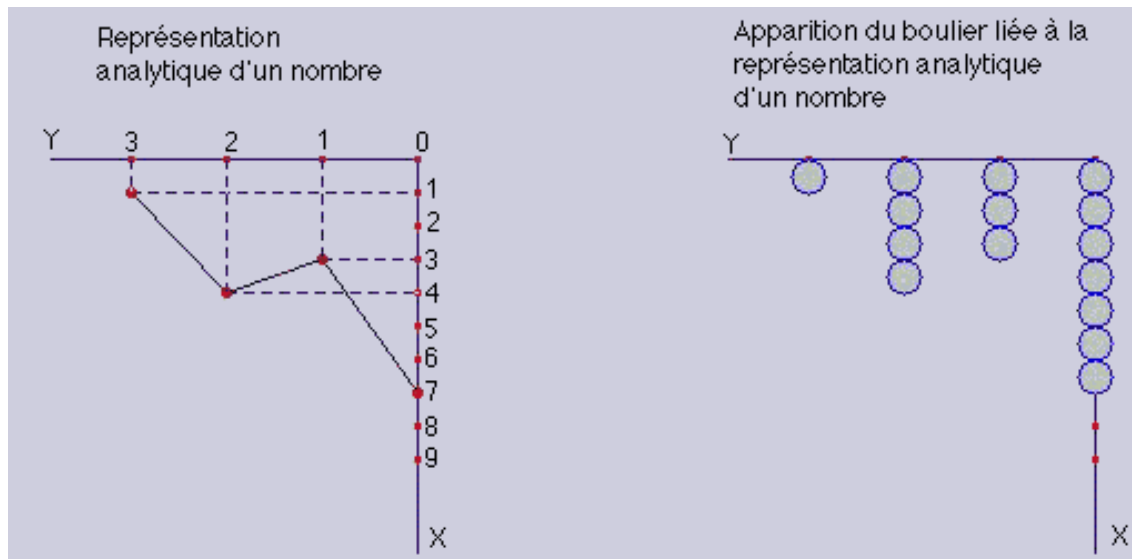


FIGURE 5 – Représentation analytique d'un nombre.

☞ La mécanographie

☞ Le boulier chinois (ou abaque)

Les premiers bouliers seraient apparus vers l'an 300 av. J.-C. en Asie (Fig. 6). Ce sont des appareils purement mécaniques directement inspirés du système de numération de position tel qu'illustré à la Fig. 5.

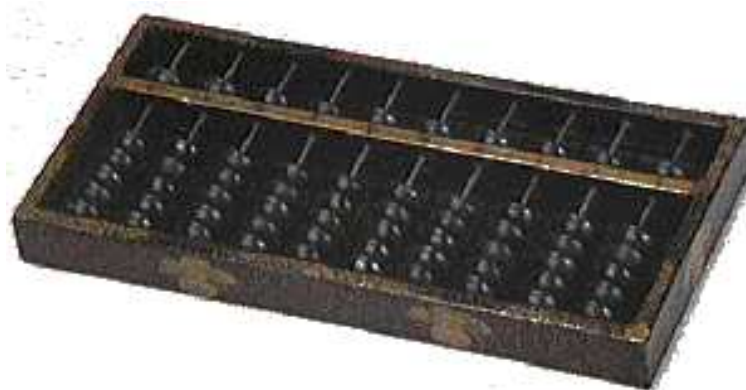


FIGURE 6 – Photo d'un boulier.

L'abaque (appelé *soroban* au Japon) est considéré comme le deuxième outil (après le couteau et avant le compas) le plus important de tous les temps en terme d'impact sur la civilisation humaine. En effet, l'abaque a été et est encore dans certains pays un outil pour aider l'être humain à effectuer rapidement ses calculs, que ce soit dans le monde du commerce ou de l'ingénierie.

- ☛ **Wilhelm Schickard** (22 avril 1592 - 24 octobre 1635) était un scientifique allemand polyvalent considéré comme le père de la première véritable machine à calculer construite en 1623 (Fig. 7). Composée de 6 cylindres Népériens, de réglettes coulissantes et de 6 disques opérateurs, la machine de Schickard était capable d'effectuer les reports de retenues dans un sens (**addition**) ou dans l'autre (**soustraction**). Détruite en 1624, elle ne sera reconstruite qu'en 1960 d'après les plans originaux.



FIGURE 7 – La machine à calculer de Schickard (1623).

- ☛ **Blaise Pascal** (19 juin 1623 - 19 août 1662) était un mathématicien et physicien, philosophe, moraliste et théologien français qui construit à l'âge de 18 ans la **Pascaline** (Fig. 8). Les roues dentées qui la constituent comportent 10 positions (de 0 à 9). À chaque fois qu'une roue passe de la position 9 à la position 0, la roue immédiatement à sa gauche, avance d'une position. Elle permet de faire les quatre opérations (addition, soustraction, multiplication, division).
- ☛ **Gottfried Wilhelm von Leibniz** (1^{er} juillet 1646 - 14 novembre 1716) était un philosophe, scientifique, mathématicien, diplomate, bibliothécaire et homme de loi allemand. Il a amélioré la machine à calculer de Pascal et a fondé les bases de l'**arithmétique binaire**. Il fut en effet le premier à comprendre l'intérêt de la numération binaire pour le calcul automatique.
- ☛ **Charles Babbage** (26 décembre 1791 - 18 octobre 1871) était un mathématicien, philosophe, inventeur et ingénieur mécanique anglais, à l'origine du concept d'**ordinateur programmable**. En 1834, il entreprend la construction de la « machine analytique » (Fig. 9), une grande calculatrice programmable universelle, grâce à l'utilisation de **cartes perforées**. Il avait déjà émis les notions de **processeur**, de **mémoire**, d'**entrées-sorties** et de **programmes**.

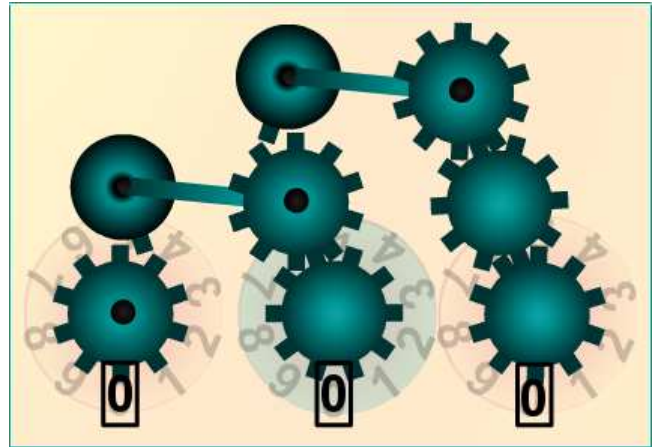
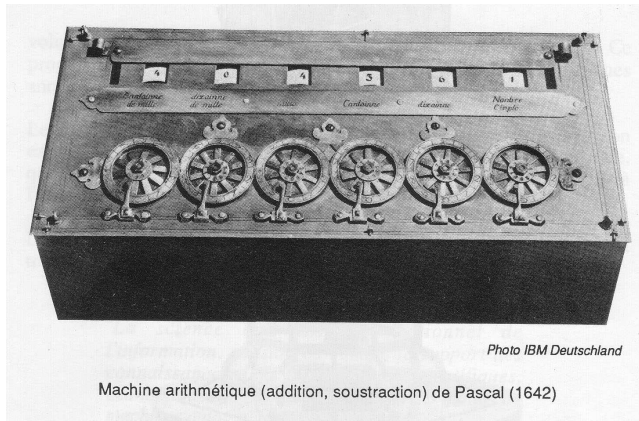


FIGURE 8 – La pascaline (1642) et son fonctionnement.

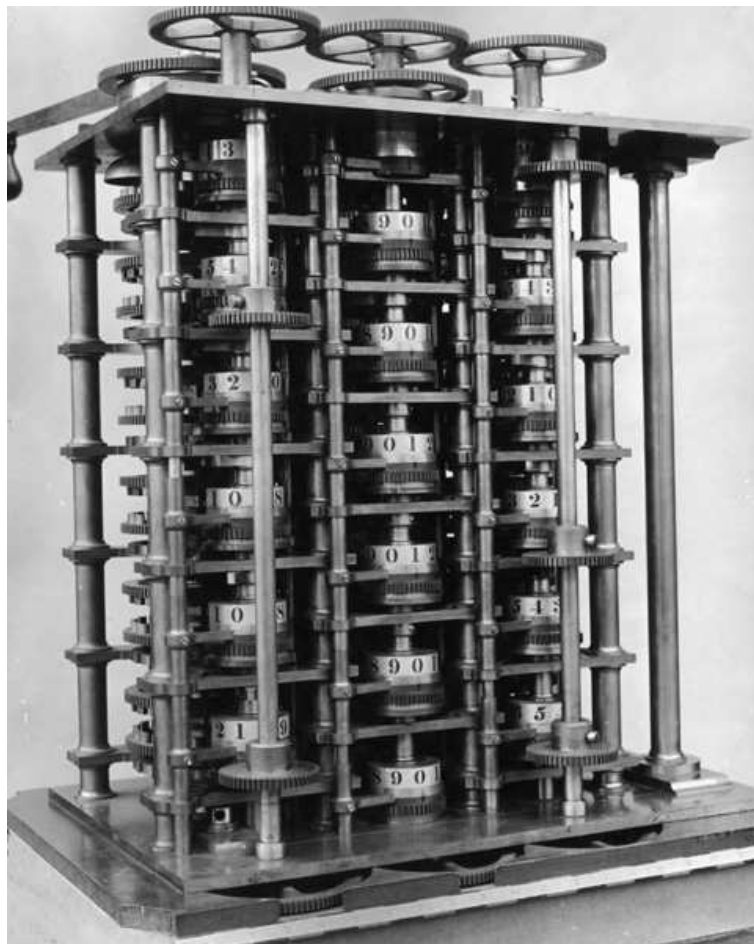


FIGURE 9 – La machine à calculer de Babbage (1834).

✦ **Ada Lovelace** (10 décembre 1815 - 27 novembre 1852) était une brillante mathématicienne anglaise connue pour avoir aidé Babbage à établir une description de sa machine analytique.

Entre 1842 et 1843, elle passa neuf mois à traduire pour Babbage (depuis le français) le mémoire du mathématicien italien Federico Luigi sur la machine analytique. Elle *aurait* ajouté à cet article plusieurs notes qui mentionnaient une méthode très détaillée pour calculer les nombres de Bernoulli

avec la machine analytique. Ces notes sont considérées par les historiens comme le **premier programme informatique au monde**.

- ☛ **George Boole** (2 novembre 1815 - 8 décembre 1864) était un logicien, mathématicien et philosophe anglais. Il est connu comme le créateur de la logique moderne, fondée sur une structure algébrique définissant une sémantique, que l'on appelle **algèbre de Boole** (ouvrage complet publié en 1854 : *An Investigation into the Laws of Thought, on Which Are Founded the Mathematical Theories of Logic and Probabilities*).

L'algèbre de Boole est la partie des mathématiques, de la logique et de l'électronique qui s'intéresse aux **opérations et aux fonctions sur les variables logiques**.

- ☛ **Herman Hollerith** (29 février 1860 - 17 novembre 1929) était un statisticien germano-américain connu pour avoir construit en 1890 une **machine mécanique programmable** à base de cartes perforées afin d'accélérer les calculs du recensement américain. Il fonda la *Tabulating Machines Company* qui devient en 1924 **IBM** (*International Business Machines Corporation*). La Fig. 10 montre une carte perforée utilisée dans la machine d'Hollerith.

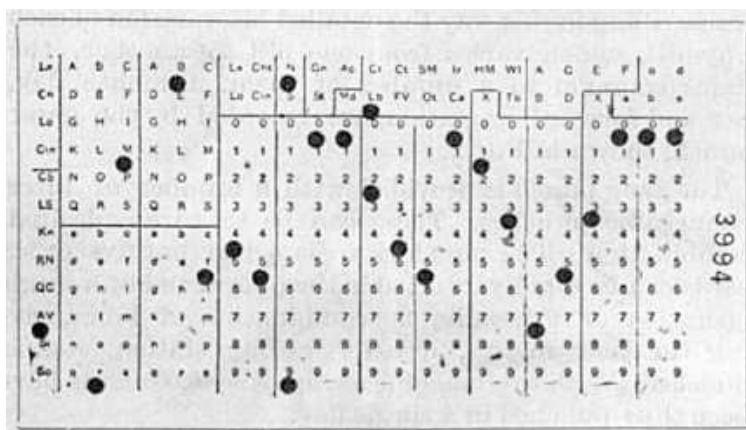


FIGURE 10 – Une carte perforée de Hollerith.

- ☛ **Vannevar Bush** (1890 - 1974) était un ingénieur américain qui a développé avec ses collègues un **analyseur différentiel** (AD), calculateur analogique dont les systèmes de roues et de volants pouvaient résoudre, grâce à des méthodes d'intégration, des équations différentielles de différents ordres (Fig. 11).

Les équations différentielles jouent un rôle essentiel en physique, chimie, économie et bien d'autres disciplines.

- ☛ **Claude Shannon** (30 avril 1916 - 24 février 2001) était un ingénieur électricien et mathématicien américain. Il est considéré comme l'un des pères, sinon le père fondateur, de la **théorie de l'information**. Il étudie entre autres l'algèbre de Boole à l'université du Michigan pour sa maîtrise soutenue en 1938 au MIT (*Massachusetts Institute of Technology*). Il y explique comment construire des **machines à relais en ' utilisant l'algèbre de Boole pour décrire l'état des relais (1 : fermé, 0 : ouvert)**. Il



FIGURE 11 – Analyseur différentiel au *Lewis Flight Propulsion Laboratory* en 1951.

est donc le premier à faire le **lien entre nombres binaires, algèbre booléenne et circuits électriques**.

- ☛ **Konrad Zuse** (Berlin, 22 juin 1910 - Hünfeld, 18 décembre 1995) était un ingénieur civil allemand et un des pionniers de l'informatique. Sa plus grande réalisation a été de concevoir et construire le **premier calculateur binaire universel programmable** (par cartes perforées) basée sur le modèle de la **machine de Turing**, le **Z3**, achevé en 1941 (Fig. 12).

Le programme d'entrée était inscrit sur un film photographique 35mm perforé. Le programme **encodait** toutes les opérations arithmétiques et les opérations d'entrée et de sortie de l'unité de mémoire et contenait une commande FIN pour arrêter la machine. L'utilisateur pressait alors une touche de conversion pour transformer le résultat binaire en décimal. Bien que Zuse souhaitait avoir une mémoire de 1024 nombres, les nécessités budgétaires et de rapidité de construction l'obligèrent à se limiter à **64 nombres**. Le Z3 était aussi la première machine à utiliser le concept d'**arithmétique flottante** où l'on utilise une notation avec un exposant pour déterminer la position de la virgule.

Le Z3 et son successeur Z4 ont été utilisés essentiellement en **aéronautique**.

- ☛ La **machine de Turing** est une machine électromécanique mise au point en 1939 par le mathématicien anglais **Alan Turing** (1912 - 1954) (Fig. 13). Cette machine a été conçue sur le plan théorique pour résoudre tout problème mathématique sous forme d'algorithme. En pratique, Turing l'a utilisée pour déchiffrer les codes secrets des Nazis pendant la seconde guerre mondiale.

- ☛ **Howard Aiken** (8 mars 1900 - 14 mars 1973) était également un ingénieur pionnier de l'informa-

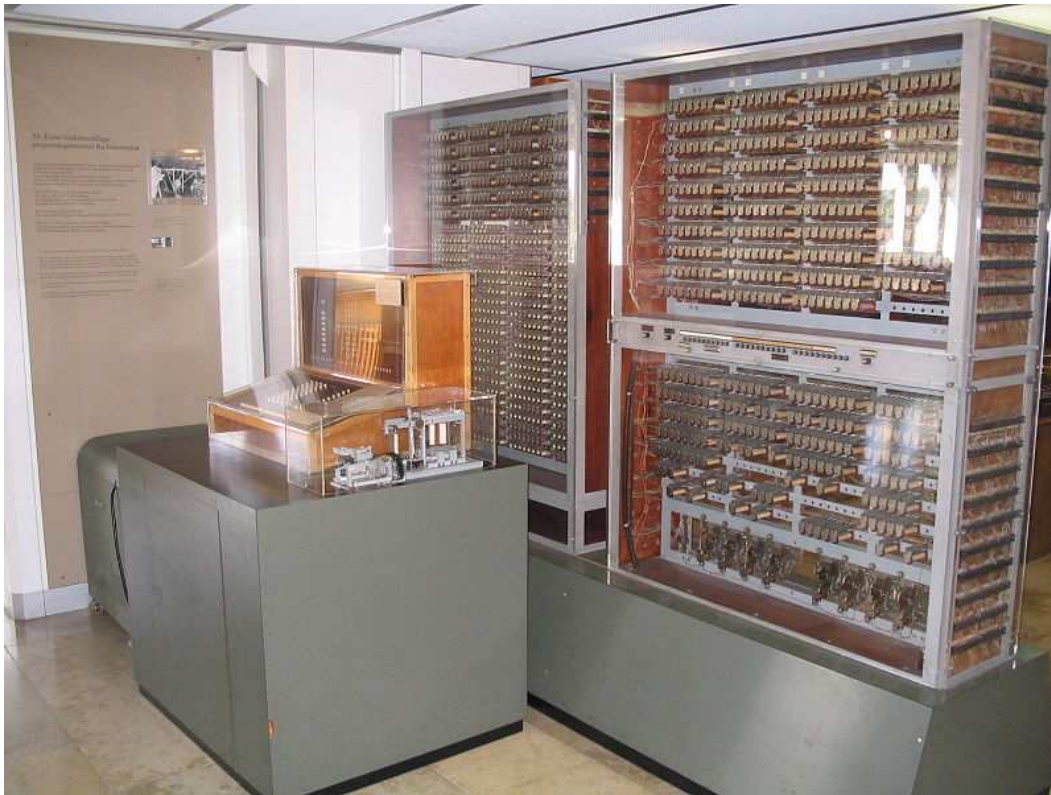


FIGURE 12 – Une réplique du fameux Z3.

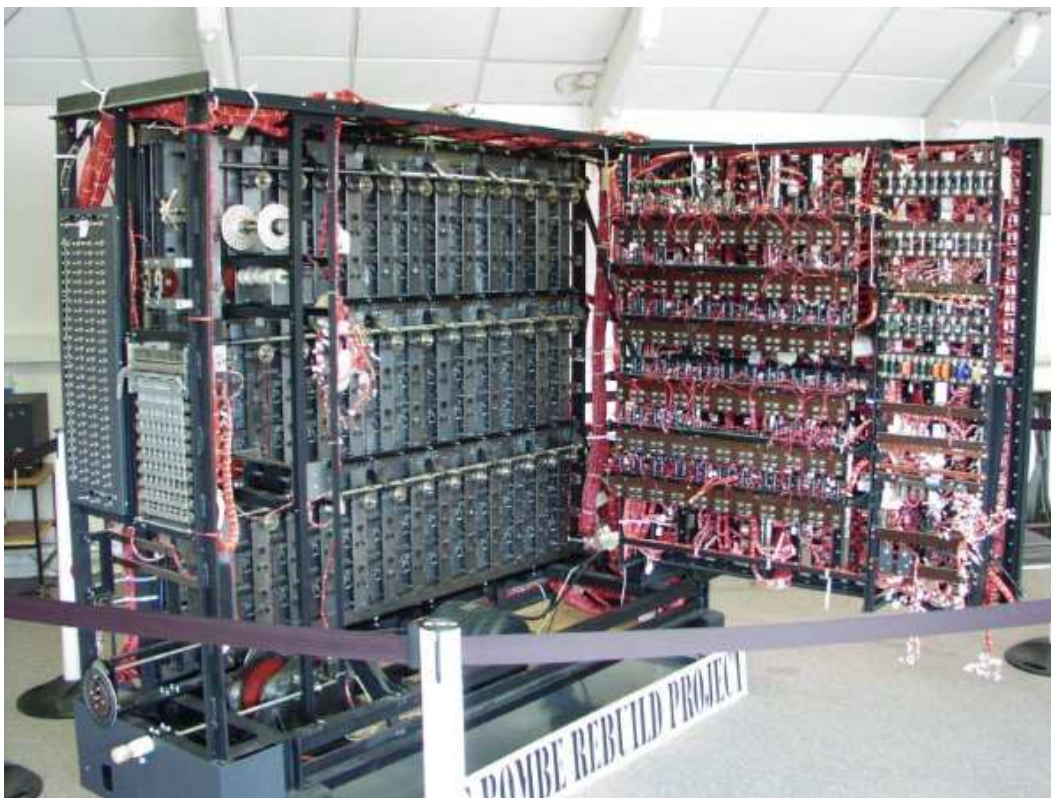


FIGURE 13 – La machine de Turing, surnommée la « bombe ».

tique, connu notamment pour avoir été l'initiateur de la construction du **premier ordinateur IBM**, le **Mark1**, sorti en 1944 (construit en 5 ans).

Le Mark1 était une énorme machine électromécanique (tubes à vide) (Fig. 14) qui pouvait fonctionner **automatiquement**, sans aucune intervention humaine, une fois son « programme » démarré. Il était aussi beaucoup plus fiable (*mean time before failure*) que ses prédécesseurs. Le Mark1 effectuait la multiplication de deux nombres de 23 chiffres en 6 secondes et l'addition et la soustraction en 3 dixièmes de seconde.

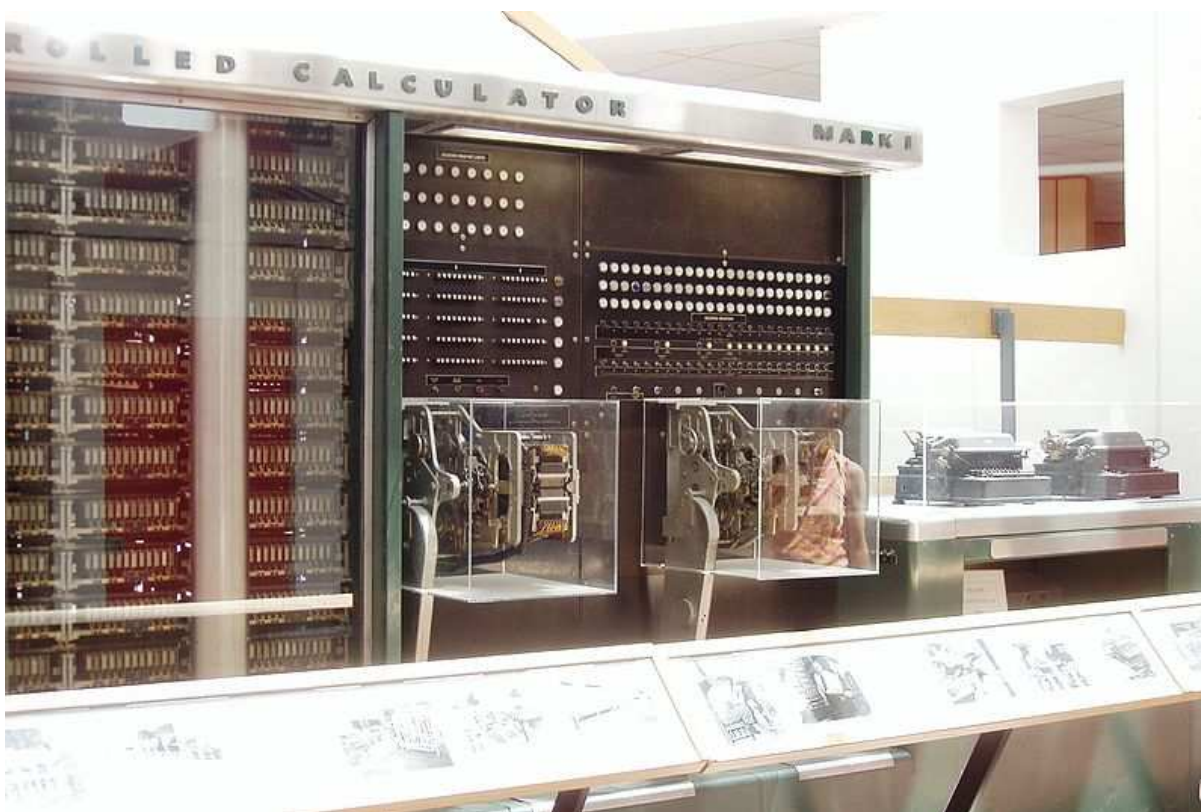


FIGURE 14 – Une partie du Mark1 d'IBM.

☛ De 1943 à 1945, **John Mauchly**, professeur de physique à l'université de Pennsylvanie, et **Presper Eckert**, jeune étudiant brillant passionné d'électronique, se consacrent à la construction d'une machine à calculer électronique pour l'armée américaine : l'**ENIAC** (*Electronic Numerator, Integrator, Analyser and Computer*) (Fig. 15).

L'ENIAC est considéré comme le premier ordinateur entièrement électronique et programmable. Son objectif initial était de calculer les tables de tir pour l'armée américaine. En pratique, sa première application importante a été la conception de la bombe à hydrogène.

L'ENIAC a été mis en service en 1946 et a fonctionné de façon presque permanente jusqu'en 1955. Il a coûté près de 500 000\$, était composé de 17 000 tubes à vide, de presque 5 millions de soudures à la main et pesait environ 30 tonnes.

Les entrées/sorties de données s'effectuaient à l'aide d'une machine à cartes perforées et d'un lecteur

de cartes **IBM**.

L'ENIAC était composé d'**accumulateurs** qui permettaient la mémorisation d'un nombre décimal, son effacement, sa transmission vers d'autres accumulateurs ainsi que l'ajout d'un nouveau nombre à celui en mémoire.

L'ENIAC pouvait effectuer près de 5000 additions de nombres de dix chiffres en une seconde, ou la multiplication de deux nombres de 10 chiffres en 3ms.

En 1997, des étudiants ont créé une réplique de l'ENIAC sur un seul circuit intégré !

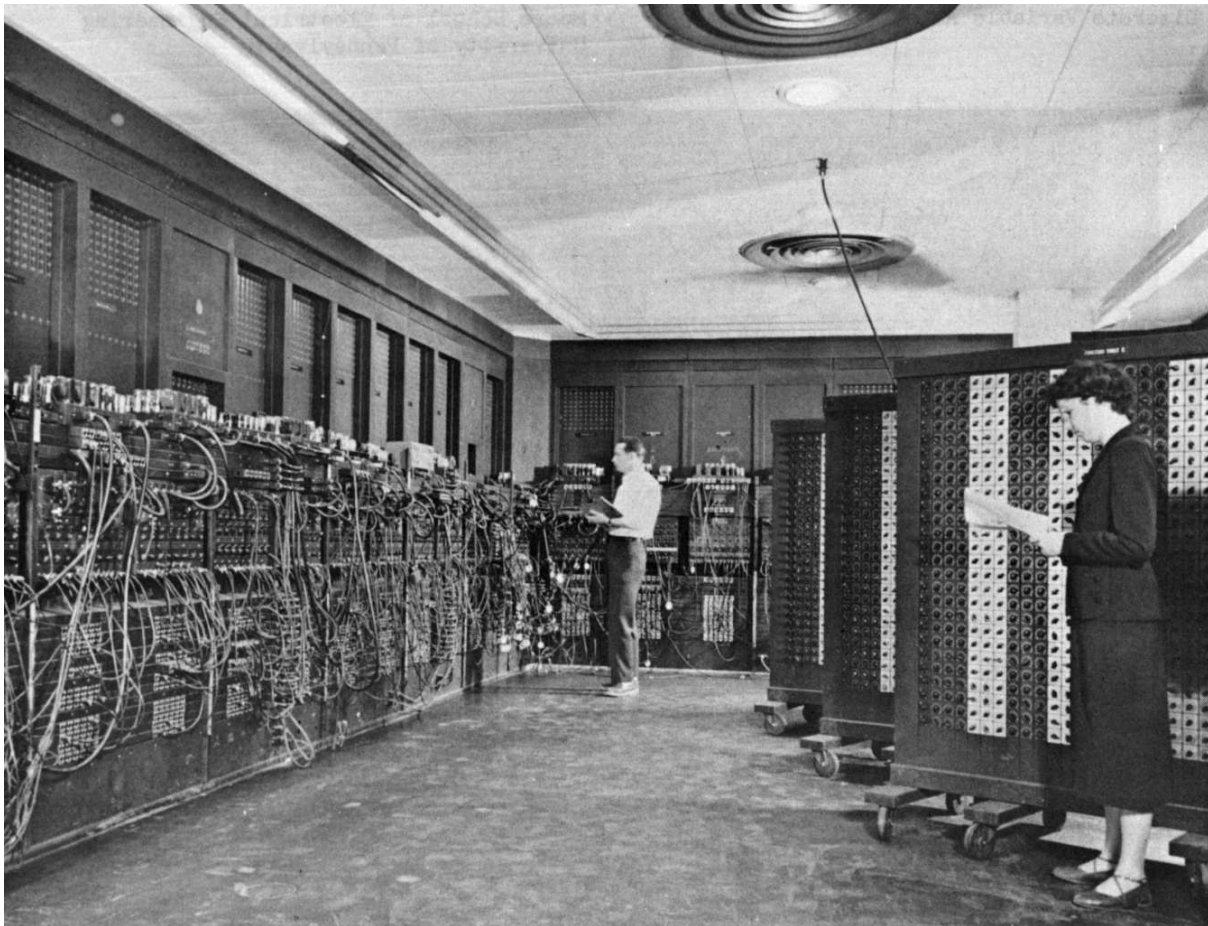


FIGURE 15 – L'ENIAC (1946).

✦ **John von Neumann** (28 décembre 1903 - 8 février 1957) était un mathématicien américano-hongrois dont les contributions ont été majeures dans divers domaines : théorie des ensembles, géométrie continue, théorie des jeux, informatique, analyse numérique, hydrodynamique, statistiques, etc. Il est considéré comme l'un des mathématiciens les plus brillants du 20^e siècle.

En se basant sur les travaux de Eckert et Mauchly sur l'ENIAC, Von Neumann eut le génie de décrire l'architecture d'un ordinateur où **données et programmes** sont adressés par des **bus d'adresses**. Il avait donc déjà conçu la notion de **programme** (instructions + données) enregistré en **mémoire**.

- La machine est contrôlée par programme
- Les instructions sont codées sous forme numérique (binaire) et enregistrées en mémoire

➤ Le programme est exécuté séquentiellement mais permet des ruptures de séquence. L'architecture comprend une **unité arithmétique et logique (UAL)**, une **unité de commande**, une **mémoire centrale**, des **unités d'entrées/sorties**.

À quelques rares exceptions, tous les ordinateurs actuels utilisent encore **l'architecture Von Neumann**.

Von Neumann est également connu pour sa conception d'algorithmes pour générer des **nombre aléatoires**. Il a implémenté sa méthode arithmétique sur l'ENIAC.

☛ **Lotfi Zadeh** (1921 -), originaire d'Iran et qui s'installa aux États-Unis en 1944, est considéré comme le père de la **logique floue**.

La logique floue est dérivée de la théorie des **ensembles flous** où les éléments ont des degrés d'appartenance à des ensembles. La logique floue a été utilisée depuis dans de nombreuses applications telles que la reconnaissance du langage (écrit ou parlé), les processus de fermentation, les systèmes de freinage antiblocage (*ABS*), le traitement du verre, les algorithmes informatiques utilisés en finance, etc.

☛ **Chiffrement à clés publiques**.

À travers l'histoire, l'être humain a toujours cherché à inventer des moyens d'envoyer des messages secrets sans utiliser de fastidieux livres de codes contenant les clés de chiffrement et de déchiffrement, et qui pouvaient tomber dans les mains ennemies.

En 1976, Whitfield Diffie, Martin Hellman et Ralph Merkle, de l'université de Stanford en Californie, ont travaillé sur une méthode de chiffrement des clés publiques pour distribuer des messages codés en utilisant une paire de clés de chiffrement : une clé publique et une clé privée. La clé privée est tenue secrète alors que la clé publique peut être largement distribuée sans danger pour la sécurité. Les clés sont associées mathématiquement mais il est impossible de déduire la clé privée de la clé publique.

En 1977, trois chercheurs du **MIT** ont suggéré l'utilisation des nombres premiers pour ce principe de chiffrement par clés. En effet, la multiplication de deux grands nombres premiers est une chose facile pour un ordinateur, mais l'opération inverse qui consiste à retrouver les deux nombres premiers à partir de leur produit est un problème très difficile.

☛ **Évolution de l'industrie informatique**

➤ **1^{ère} génération** : années 1950 → **tubes à vide**.

➤ **2^{ème} génération** : années 1960 → **transistors**.

➤ **3^{ème} génération** : années 1970 → **circuits intégrés**.

Apparition des **micro-processeurs** et des **puces électroniques**.

➤ **4^{ème} génération** : fin des années 1980.

⇒ Apparition des **ordinateurs personnels**.

⇒ Multiplication des **périphériques** : disques, imprimantes laser, écrans couleurs, etc.

⇒ Explosion des **réseaux** : câble, fibre optique, téléphone, satellite.

- **5^{ème} génération** : quand et quoi ? (Ordinateurs neuronaux ?)
 - ⇒ Recherches en **intelligence artificielle**.
 - ⇒ Objectif : utilisation toujours plus simple et plus naturelle.
 - ⇒ **Architectures parallèles, systèmes neuronaux, multiprocesseurs**.

☞ Et plus récemment, **l'histoire du Web** . . .

- ☞ **Internet** : Infrastructure mondiale constituée d'un ensemble de réseaux nationaux, régionaux et privés, reliés par le protocole de communication TCP/IP.
- ☞ **World Wide Web** : sous-réseau de l'Internet utilisant le protocole **HTTP** (*HyperText Transfer Protocol*).
- ☞ **Quelques dates et noms clés** :
 - **1950** : Langages hypertextes et développements théoriques (**Ted Nelson**).
 - **1969** : Développement du GML (*Generalized Markup Language*) par **IBM**.
 - **1989** : Projet au **CERN** (anciennement Conseil Européen pour la Recherche Nucléaire, Genève, Suisse) pour développer une technologie d'échange d'information entre ordinateurs du CERN à travers le langage **HTML** (*HyperText Markup Language*). Projet soumis par le physicien **Tim Berners-Lee**.
 - **1990** : Premier prototype **WWW**.
<http://info.cern.ch/hypertext/WWW/TheProject.html>
 - **1991** : Lancement officiel du Web (`alt.hypertext`) et premier navigateur en mode texte. Première version de **HTML** (*HyperText Markup Language*) : **HTML 1.0**.
 - **1992** : Premiers navigateurs graphiques (ERWISE, VIOLAWWW, LYNX).
 - **1993** : MOSAIC
 - **1994** : NETSCAPE NAVIGATOR. **HTML 2.0**.
 - **1995** : Fondation du **W3C** (*World Wide Web Consortium*), toujours dirigé par Tim Berners-Lee. Le W3C développe des standards ouverts pour améliorer l'interopérabilité du Web ((X)HTML, XML, CSS, XSL, SVG, SSML, SMIL, etc.).

I.2. Rôles et organisation de la recherche

Depuis une trentaine d'années, dans le monde académique universitaire, un proverbe anglais bien connu est devenu lieu commun : « Publish or perish » . . . avec les avantages et les inconvénients que cela pose.

I.2.1. Rôle de la recherche dans l'éducation post-secondaire

De manière générale, **la recherche réhausse la qualité de l'enseignement** (gradué ou sous-gradué) en y apportant des mises à jour fréquentes sur l'état de l'art d'un domaine scientifique, et donc améliore au fil des années la qualité des diplômes offerts aux étudiantes et étudiants.

Au niveau de la **maîtrise**, l'étudiante ou l'étudiant doit approfondir un sujet spécifique et être capable d'apporter des **innovations** au sujet. Cependant on ne s'attend pas à ce que l'étudiante ou l'étudiant soit