

Histoire de l'informatique

Frédéric Gava (MCF)

gava@univ-paris12.fr

LACL, bâtiment P2 du CMC, bureau 221

Université de Paris XII Val-de-Marne

61 avenue du Général de Gaulle

94010 Créteil cedex



Définition

Informatique = Information + Automatique

Ce terme a été introduit en France. Il est très répandu dans le monde à part dans les pays **anglo-saxons** où le terme dominant est *computer science*.

Informatique = Théories et des supports physiques

Un **ordinateur** est un ensemble de dispositifs mécaniques, électroniques et logiciels capable de réceptionner, de traiter et d'émettre de l'information.

Frise chronologique

Théories



**-30000 ans
entailles**

Supports physiques

La plus grande idée...



Os avec des nombres : - 8500

Première arithmétique

Des entailles sont **efficaces pour l'arithmétique** :

$$\text{|||||} + \text{|||} = \text{|||||||} \quad (7+3 = 10)$$

$$\text{|||||} * \text{|||} = \text{|||||||} \quad (7 * 3 = 21)$$

Mais **inefficaces pour la représentation et la sauvegarde**

cent en **décimal** et cent en **entailles**

100



Puis vint le Signe !

Frise chronologique

Théories

**-3000
les numérations**








**-1500
les bases**



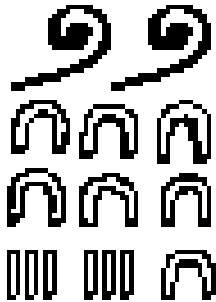
**-30000
entailles**

Supports physiques

Première numération

						
1	10	100	1000	10000	100000	10^6

























Egypte -3000


276


































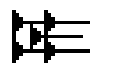



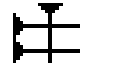

































































L'arithmétique y est difficile

Et pour la langue...

				
<i>hr</i>	<i>pr</i>	<i>rʿ</i>	<i>s3</i>	<i>iw</i>
'head'	'house'	'sun', 'day'	'duck'	'to walk'

glyph	translit.	phonetic	glyph	translit.	phonetic
	<i>3</i>	[ʔ]		<i>h</i>	[h]
	<i>t</i>	[t]		<i>h</i>	[x]
	<i>y</i>	[y]		<i>h</i>	[ç]
	<i>ʿ</i>	[ʿ]		<i>s</i>	[s]
	<i>w</i>	[w]		<i>š</i>	[š]
	<i>b</i>	[b]		<i>k</i>	[q]
	<i>p</i>	[p]		<i>k</i>	[k]
	<i>f</i>	[f]		<i>g</i>	[g]
	<i>m</i>	[m]		<i>t</i>	[t]
	<i>n</i>	[n]		<i>t</i>	[tʰ], [c]
	<i>r</i>	[r]		<i>d</i>	[d]
	<i>h</i>	[h]		<i>d</i>	[dʰ], [ɹ]

UGARITIC AND PHOENICIAN ALPHABETS COMPARED TO ACCADIAN AND SINAI SIGNS

<i>Accadian</i>	<i>Ugaritic</i>	<i>Phoenician</i>	<i>Sinai</i>	<i>Accadian</i>	<i>Ugaritic</i>	<i>Phoenician</i>	<i>Sinai</i>
 a	 'a	 'a	 'a	 šu	 d		
 bi	 b	 b	 b	 na	 n	 n	 n
 gi	 g	 g	 g	 su	 z		
 ha	 h			 ša	 s	 s	
 da	 d	 d	 d	 ha	 'a	 'a	 'a
 he	 h	 h	 h	 pa	 p	 p	 p
 wa	 w	 w	 w	 ša	 š	 š	 š
 za	 z	 z	 z	 qa	 q	 q	 q
 ha	 ḥ	 ḥ	 ḥ	 ra	 r	 r	 r
 tî	 t	 t	 t	 tî	 t	 š	 š
 ya	 y	 y	 y	 ga	 ḡ		
 ka	 k	 k	 k	 ti	 t	 t	 t
 ša	 š			 e	 'i,e		
 lu	 l	 l	 l	 u	 'u,o		
 ma	 m	 m	 m	 se	 š		<i>Beta</i>

La première base (1)

1		11		21		31		41		51	
2		12		22		32		42		52	
3		13		23		33		43		53	
4		14		24		34		44		54	
5		15		25		35		45		55	
6		16		26		36		46		56	
7		17		27		37		47		57	
8		18		28		38		48		58	
9		19		29		39		49		59	
10		20		30		40		50			

59 symboles pour le système **Babylonien**.

Il n'y a pas zéro !

La première base (2)

- **Systeme sexagésimal Babylonien : entre -1900 et -1500**
- **Le premier système positionnel connu (la valeur d'un chiffre dépend de sa position)**
- **Les chinois utilisaient un système positionnel en -1300**

Comment distinguer 1 et 60 ? A l'aide du contexte. Finalement un symbole pour une position a été introduit, mais n'était pas considéré comme un chiffre.

Pour calculer les sommes et les produits assez vite il faut connaître les tables de l'addition et de la multiplication. Pour le système sexagésimal ils sont trop grands (il y a 58 nombres non triviaux : 2, 3, ... , 58; la taille de la table est 3364).

Mais on peut utiliser différents trucs pour réduire les tables, par exemple $58 \cdot 58 = (68-2) \cdot (68-2) = 60^2 - 4 \cdot 60 + 4$

Puis vint la machine !

Frise chronologique

Théories

**-3000
les numérations**

**-1500
les bases**

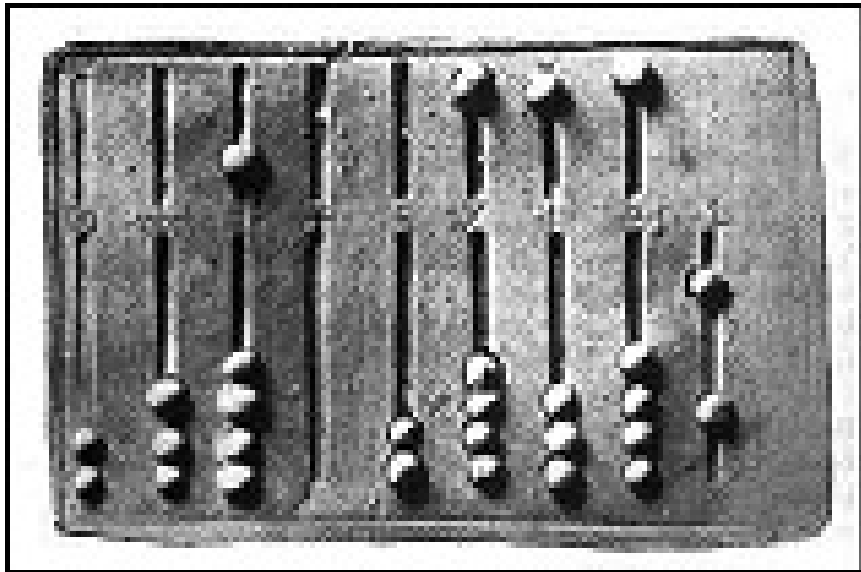


**-30000
entailles**

**-1000
le boulier**

Supports physiques

L'abaque



Inventé par les Babyloniens entre -1000 et -500 (peut-être avant par les chinois ?)

Puis vint le
raisonnement !

Frise chronologique

Théories

**-3000
les numérations**

**-1500
les bases**

**-300
la logique**



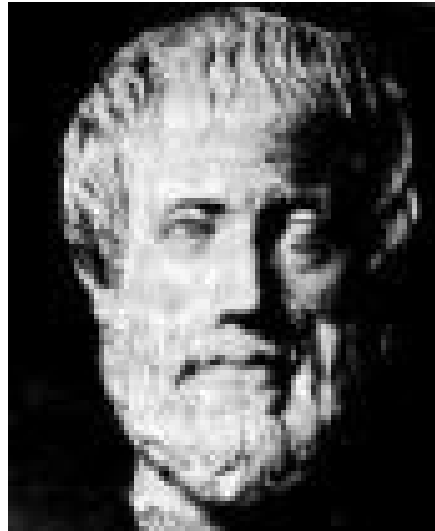
**-30000
entailles**

**-1000
le boulier**

Supports physiques

La logique

Aristote
-384 → -322



Le **traitement** de l'**information** ne se réduit pas au **calcul**. On la **sauvegarde**. On la **transforme**. On **raisonne**.

Raisonner suppose une **logique** :

- Théorie de l'inférence = **sylogistique**
- Notions d'**induction** et de **déduction**

Première application

La cryptographie

- A part le calcul numérique, l'informatique a été fortement stimulée par la **sécurité de l'information**.
- Certains moyens de sécurisation de l'information ont été utilisés depuis les temps anciens, à savoir la **stéganographie** et la **cryptographie**.
- La **stéganographie** étymologiquement veut dire **écriture cachée**.

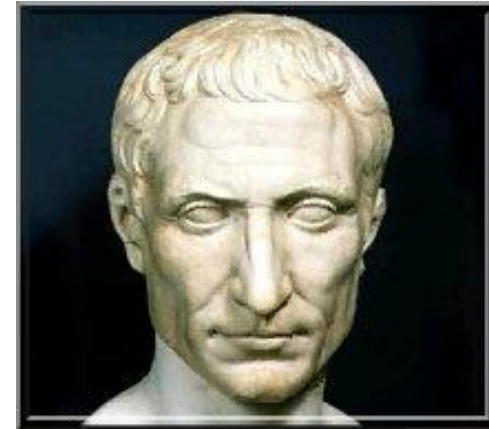
Premières méthodes

- Dans ses *Histoires*, Hérodote (486-425 BC) raconte comment vers **440 BC** on rase la tête d'un esclave, puis on y tatoua un message qui devint invisible après que les cheveux aient repoussé. Le but était de lancer une révolte contre les Perses.
- Énée le Tacticien (env. 350 BC) proposa de **cacher** un message dans un autre texte **en changeant la hauteur des lettres** ou **en perçant des petits trous au dessus** ou **en dessous des lettres** du message de couverture.
- Cette technique, toujours utilisée au 17ème siècle, fut améliorée par Wilkins qui utilisa des encres invisibles pour inscrire ces petits points au lieu de faire des trous. Cette dernière idée fut reprise par les espions allemands durant les deux guerres mondiales.

Le chiffrement

Jules César (Caius Julius Caesar)

-100 → -44



César utilisait un chiffrement de substitution qui décale les lettres de l'alphabet :

- **Un décalage de 1 transforme « IBM » en « HAL » (nom de l'ordinateur fou dans « *2001, a space odyssey* » de Kubrick)**
- **Un décalage de 7 transforme « MOT » en « TVA »**

Puis vint le zéro !

Frise chronologique

Théories

**500
le 0**

**800
Formalisation
des nombres**



Supports physiques

Premières formalisations

Abu Abdullah Muhammad bin Musa **al-Khwarizmi**

780 → 850

■ **830** : livre sur les mathématiques “*al-Kitab al-mukhtasar fi hisab al-jabr wa'l-muqabala*” ≈ “Le livre abrégé sur le calcul par achèvement et mise en équilibre”.

■ **825** : “Sur le calcul avec les nombres hindous” (Kitab al-Jam'a wal-Tafreeq bil Hisab al-Hindi)



Timbre-poste soviétique avec un portrait imaginé d'al-Khwarizmi

Influences

- Cela a donné, en particulier, les mots :
 - ▶ **Algorithme** qui provient du nom latinisé d'**Al-Khowarizmi**
 - ▶ **Algèbre** qui provient du nom latinisé du mot **al-jabr**
- Les livres d'Al-Khowarizmi ont été traduits ou utilisés en Europe au 12e siècle. Une contribution importante dans la dissémination de ces connaissances a été faite par **Adelard of Bath (1075 – 1160)**
- Via ces sources les nombres **décimaux** deviennent connus en Europe. Pour cette raison ils s'appellent souvent « **nombres arabes** » bien que leur origine soit **l'Inde**.

Le retour des machines

Frise chronologique

Théories

500
le 0

800
Formalisation
des nombres

1938
machine
électro-mécanique

1642
la machine
de Pascal

1800
les cartes perforées

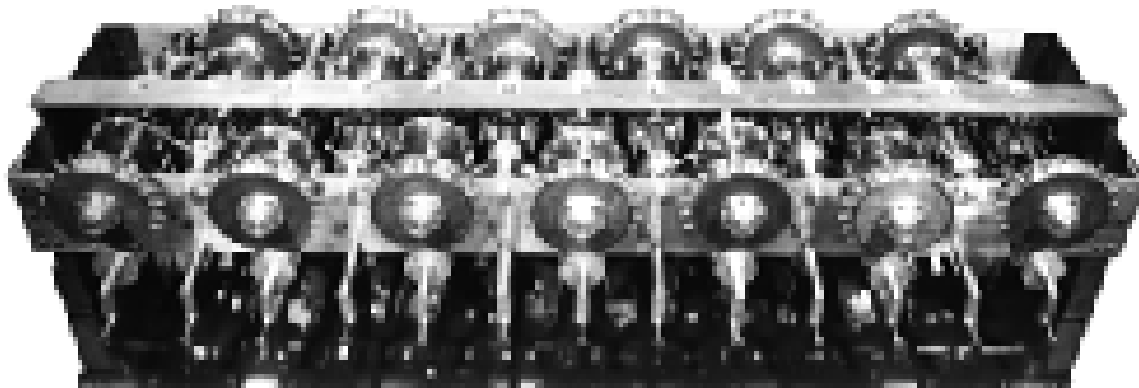
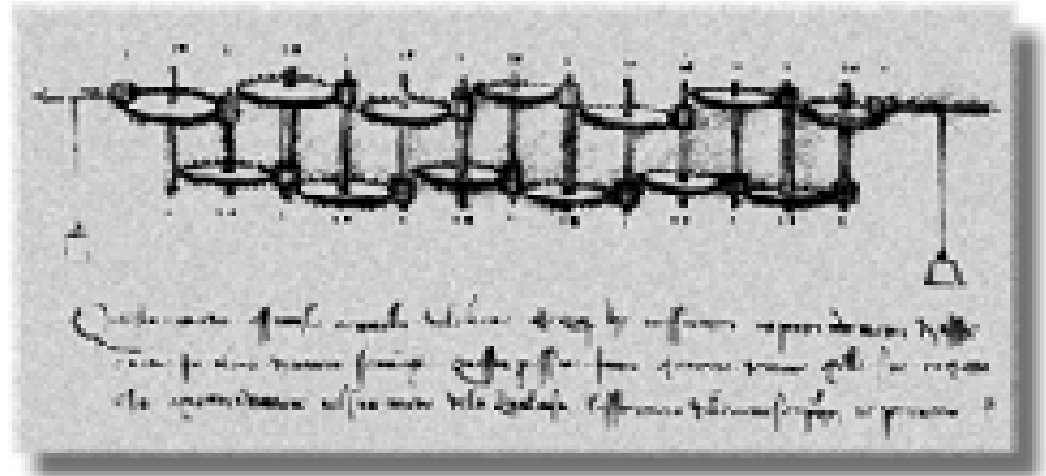
Supports physiques

Un premier essai

Léonard de Vinci
1452 → 1519



on trouve un schéma et une description
d'une machine à calculer



Un modèle fonctionnel
construit selon le schéma
de de Vinci

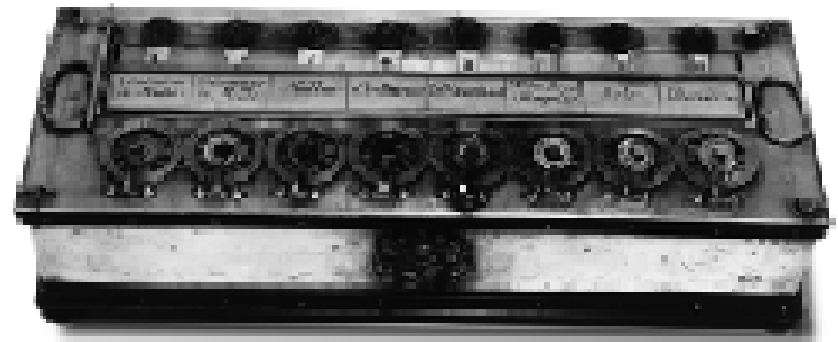
Machine arithmétique

Blaise Pascal

1623 → 1662



La première **machine mécanique** et automatique de calcul !
Faites avec des **techniques d'horlogerie**



La pascaline

- Il a produit 50 machines dans les 10 années suivantes.
- En fait, la machine de Pascal peut **additionner** directement et **soustraire** par addition du nombre **complémentaire** (comme les ordinateurs modernes). **Soustraction** par addition du nombre **complémentaire**. Exemple en base 1000 :
 - ▶ $117 - 19 = 117 + (1000 - 19)$
 - ▶ sans le chiffre gauche = $117 + 981$
 - ▶ sans le chiffre gauche = 1098
 - ▶ sans le chiffre gauche = 98.
 - ▶ Le nombre **981** est le **complément** de **19** en base 1000
- Multiplication et division étaient faites par additions et soustractions.

Les influences

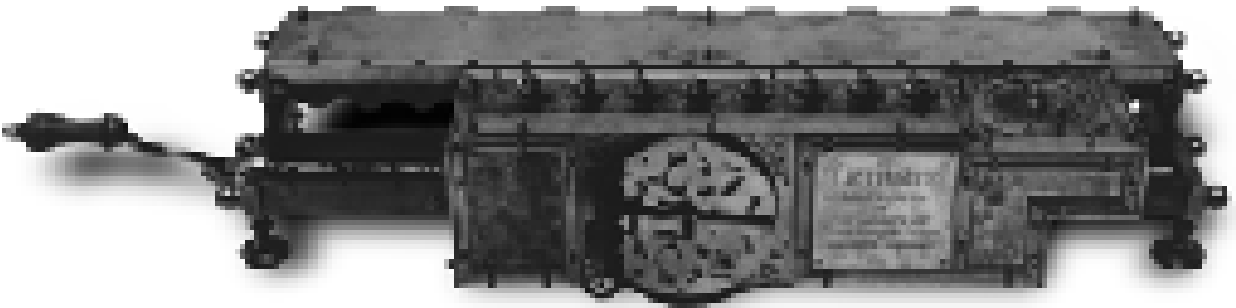
Gottfried Wilhelm Leibniz

1646 → 1716



1671 a construit le
Step Reckoner

Cette machine pouvait calculer les additions, soustractions, et aussi les multiplications, les divisions et les racines carrées par des séquences d'additions décalées.



Machines à taper (1)

- Un brevet pour un outil de ce genre a été délivré en 1714 à l'ingénieur anglais Henry Mill.
- Une des premières machines à taper commerciales a été inventée par Christopher Latham Sholes (1819-1890), ingénieur américain, brevetée en 1868.
- Il a conçu cette machine avec ses partenaires S. W. Soule and G. Glidden. La fabrication a commencé en 1873 par la Remington Arms Company

Machines à taper (2)



1870



1874



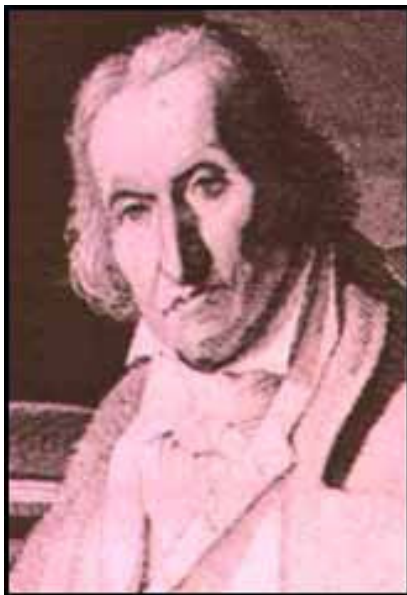
1878

Le clavier **QWERTY** a été conçu en 1868 par **Sholes**. Les **paires de lettres** les plus usitées dans la langue anglaise sont **réparties aux extrêmes** du clavier. De cette manière, la vitesse de frappe est réduite et les tiges se coincent plus rarement.

AZERTY : même considérations pour le français.

Machines dans l'industrie

Joseph Marie Jacquard
1752 → 1834



Charle Babbage
1792 → 1871

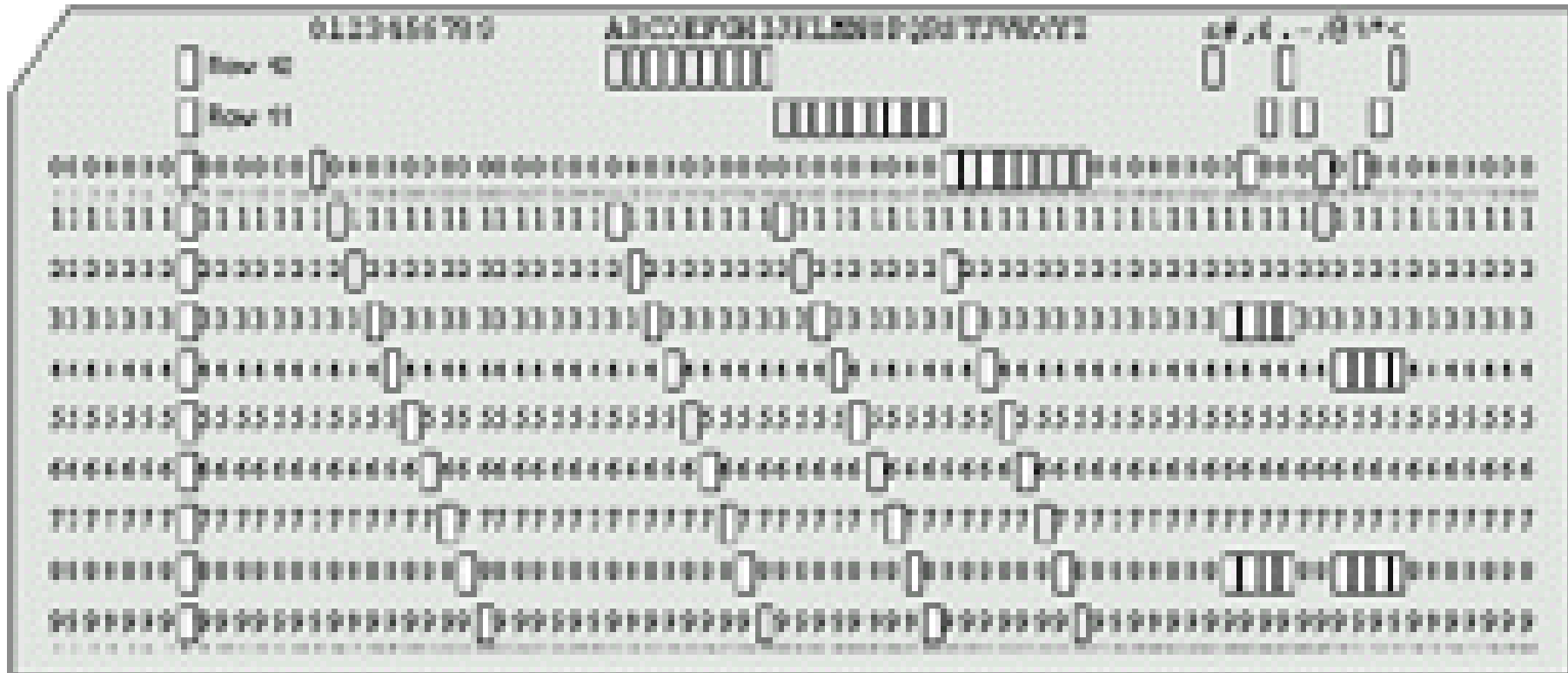


Conception des **cartes perforées** et de machines à tisser **programmables**

Machine à tisser

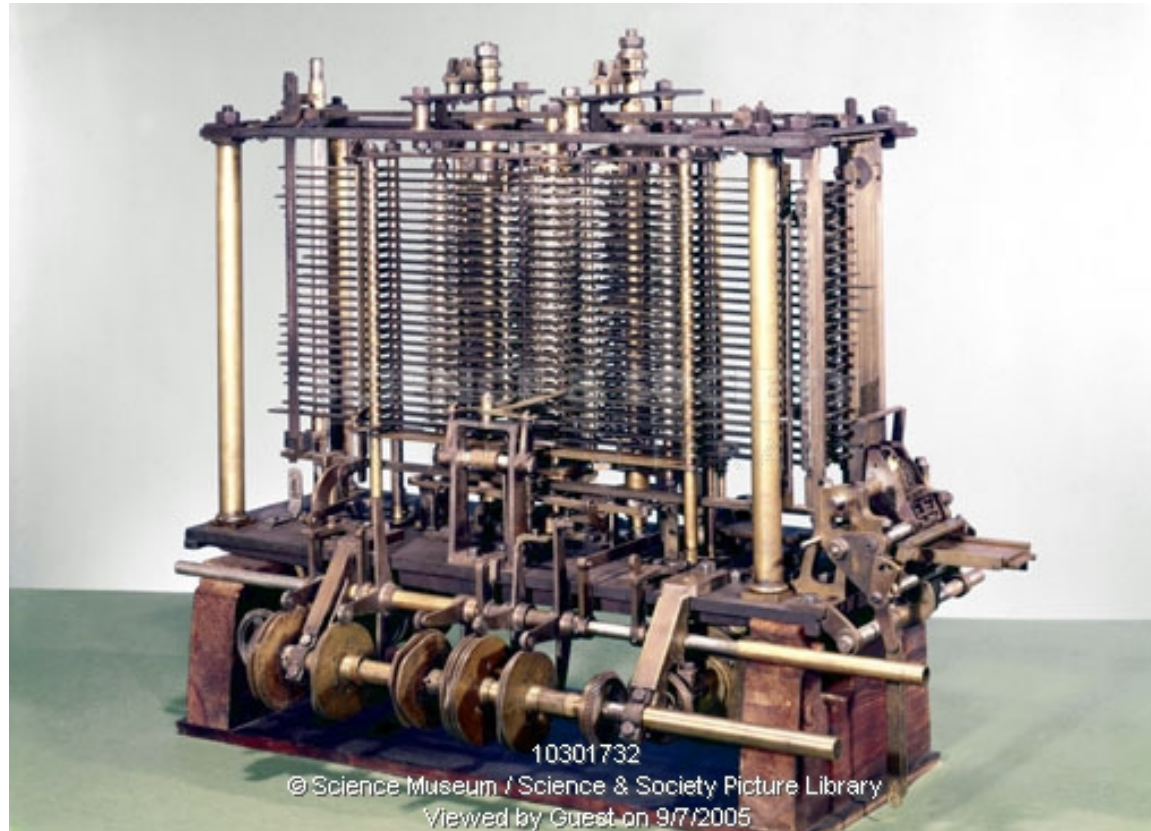


Cartes perforées



Les cartes perforées étaient utilisées pour représenter la musique pour les **pianos mécaniques**, machines de tablatures et plus tard dans les programmes pour les ordinateurs etc.

Machine de Babbage



1822, la “**Difference Engine**” puis l’idée de l’ “**Analytical Engine**” :

- Contrôle séquentiel
- Branchement
- Boucles
- Cartes perforées

La programmation

Countess Augusta Ada Lovelace

1815 → 1852



- Fille du poète Lord George Gordon **Byron**
- Brillante mathématicienne, Ada était parmi le petit nombre de personnes qui ont vraiment compris la vision de **Babbage**. Elle a programmé les premières ébauches de l'**Analytical Engin**
- Sa contribution dans le développement de l'informatique a été honorée par l'attribution de son prénom au **langage de programmation** Ada.

Le retour des Signes-logiques

Frise chronologique

Théories

1850
logique booléenne

1886
liens entre la
logique et circuits

1938
Application formelle
de la logique booléenne

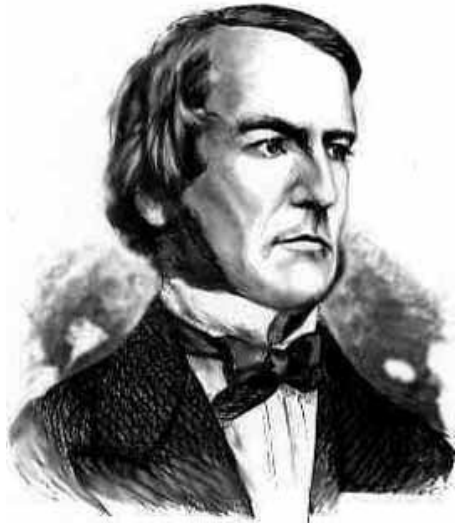
1800
les cartes perforées

1938
machine
électro-mécanique

Supports physiques

Les signes logiques

George Boole
1815 → 1864



Fondements d'une partie importante de la logique mathématique moderne (**l'algèbre de Boole**).

Vrai=1, Faux=0

Augustus de Morgan
1806 → 1871

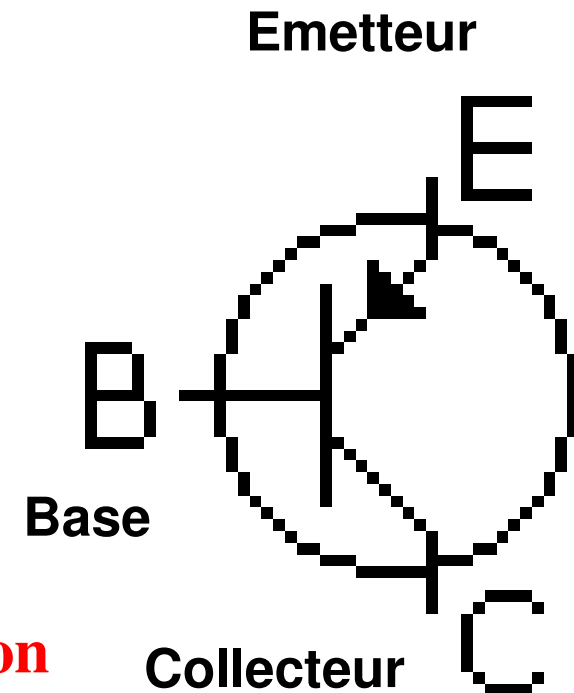
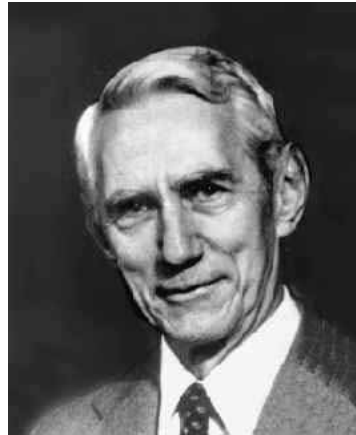


Logique des classes et des relations, il formalise un ensemble d'**opérations logiques** connues aujourd'hui comme les **transformations de De Morgan**.

$$\neg(X \wedge Y) = (\neg X \vee \neg Y)$$

Application logique

Claude Shannon
1916 → 2001



■ Formalisation et application du **lien entre l'algèbre de Boole et les circuits de commutation**

■ Notion d'entropie de l'information

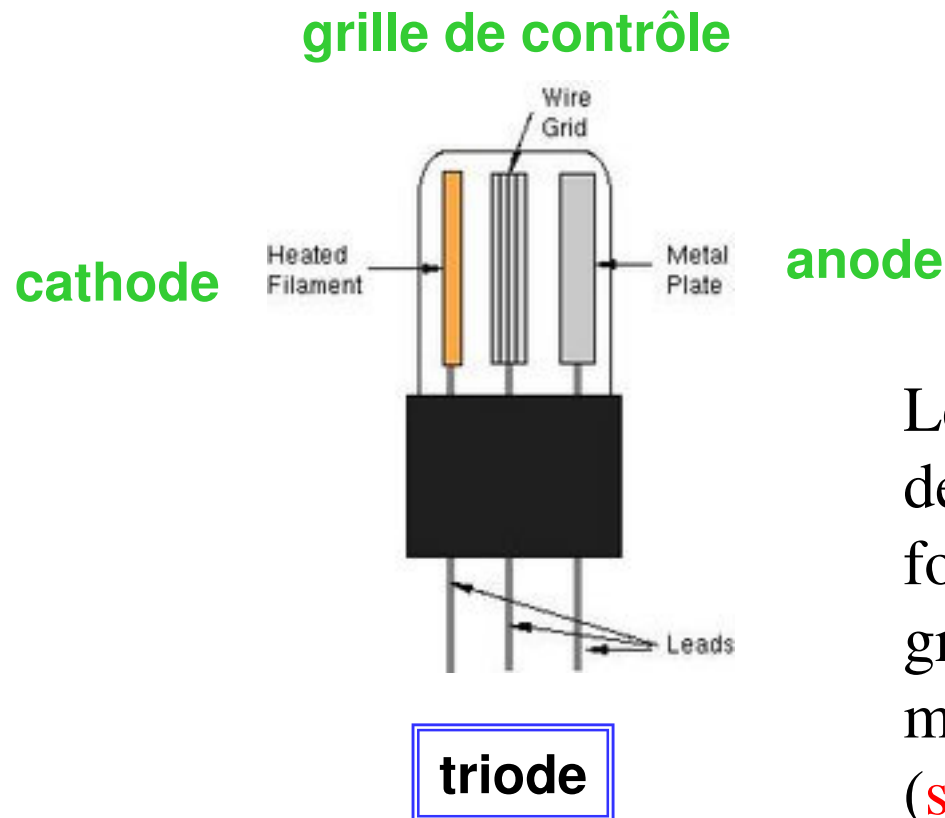
■ Système binaire : système positionnel de base 2

$$7 = 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$

La physique avance...(1)

1904: Sir John Ambrose **Fleming** (1849 - 1945), ingénieur britannique, invente la lampe à vide (diode)

1906: Lee de **Forest** construit une triode



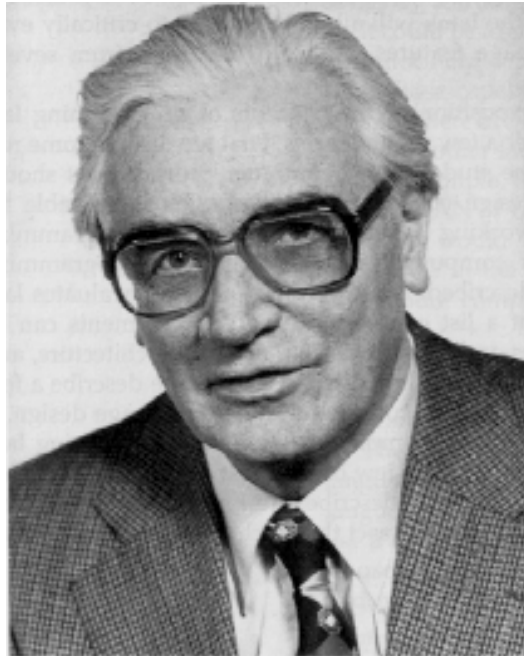
Le courant passe ou ne passe pas de la cathode à l'anode en fonction de la tension sur la grille. Ce phénomène peut modéliser une commutation (**switch**) de 2 états.

La physique avance (2)

- **1908** : Campbell **Swinton** décrit une méthode de **balayage électronique** (electronic scanning) qui présage l'utilisation du tube à **rayons cathodiques** pour la télévision
- **1915** : Manson **Benedicks** découvre que le cristal de **germanium** peut être utilisé pour convertir le courant alternatif en courant continu; cela présage les **puces (microchips)**
- **1917** : Le mot "**robot**" (dérivé du mot tchèque pour *travail*) est introduit par Karel **Čapek** (1890 - 1938) dans sa pièce de théâtre R.U.R. (Rossum's Universal Robots).

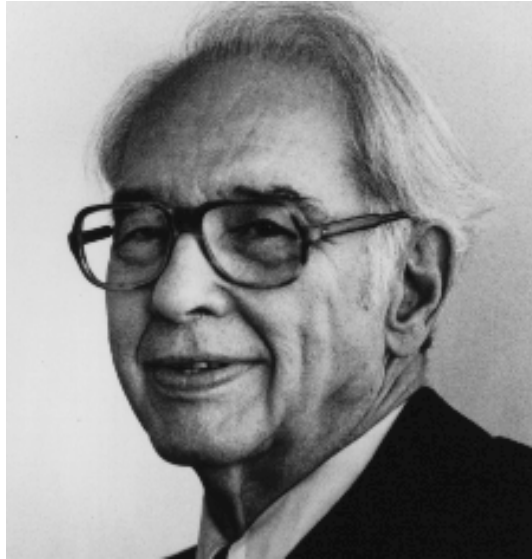
Machine électro-mécanique

Konrad Zuse
1910 → 1995



Première machine **électro-mécanique Z1** en 1938 puis un premier ordinateur (**Z3**) en 1941 qui utilisait une **numération binaire** pour les calculs en **virgule flottante**

Autres machines



John Vincent Atanasoff
(1903 - 1995)

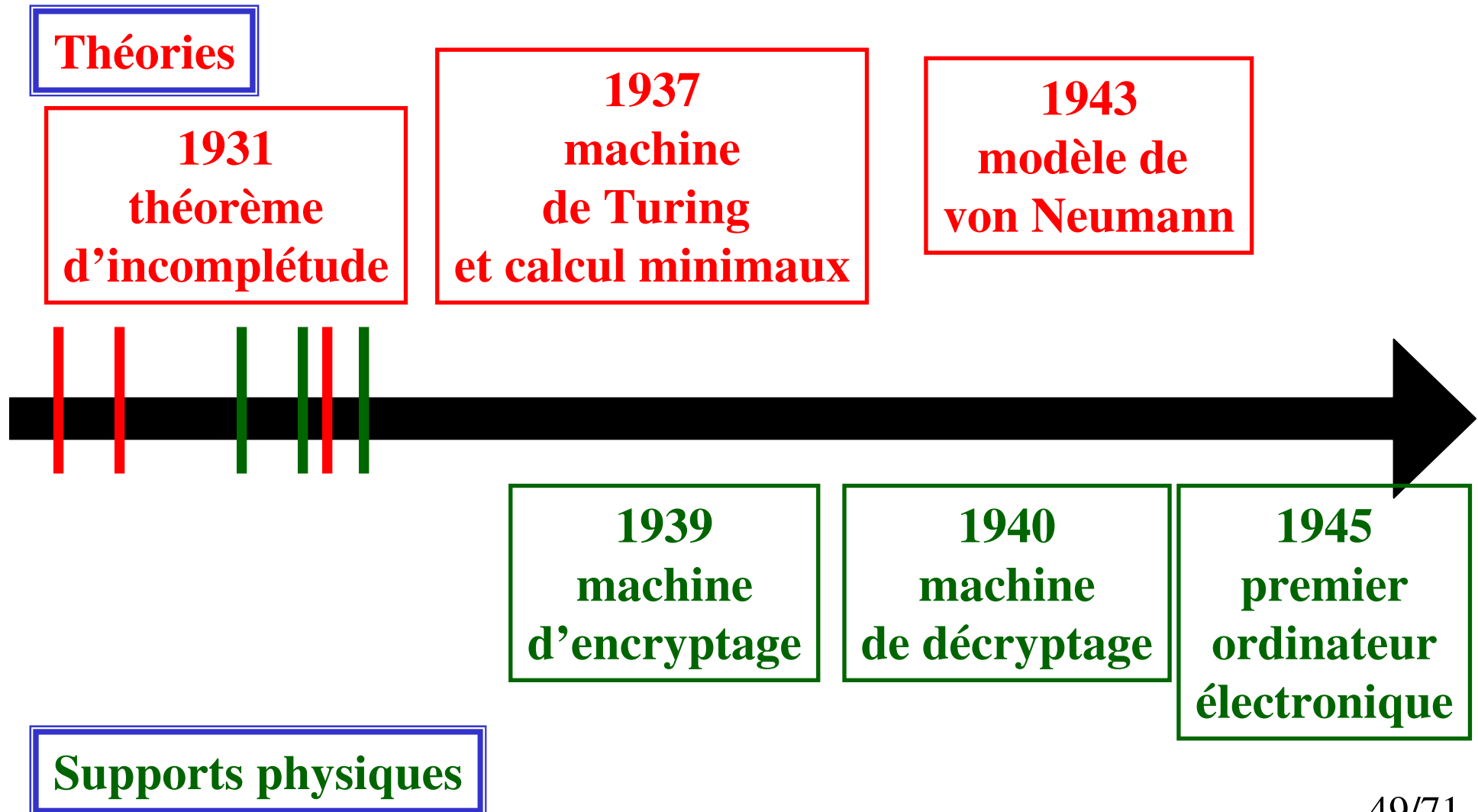


Clifford E. Berry
(1918 - 1963)

1939–1941: John Vincent **Atanasoff** et un étudiant brillant Clifford E. **Berry** développent le premier ordinateur **électronique ABC** (1939-1941). Il n'était ni universel (seulement solution des équations différentielles), ni vraiment fonctionnel.

Puis vint la révolution !

Frise chronologique



La révolution théorique

Kurt Gödel
1906 → 1978



Alonzo Church
1903 → 1995



Alan Turing
1912 → 1954



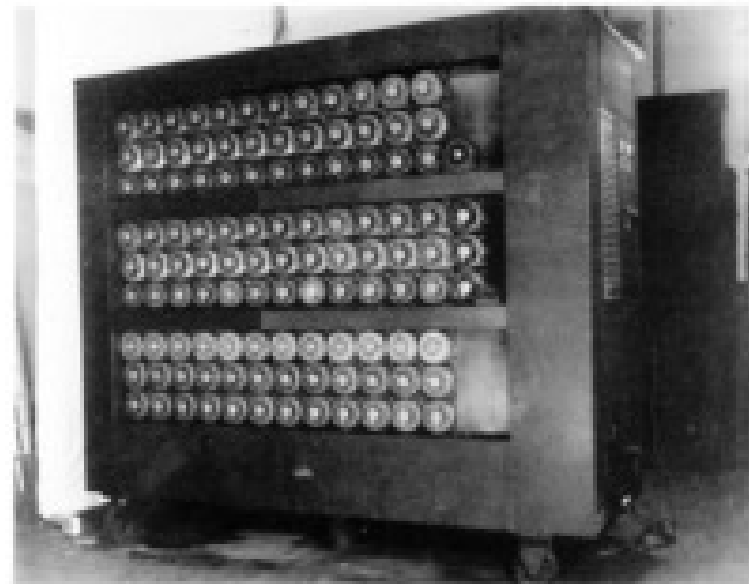
- **1931** : Théorèmes sur les problèmes des **axiomes** et de leur **complétude**
- **1936** : Conception d'un **système de calcul minimal**
- **1937** : Conception d'une **machine universelle** minimale(machine théorique);
Idée de l'**intelligence artificielle**.

La cryptographie et les machines

1939 Enigma : machine de
chiffrement allemand



1940 La Bomba : machine
électro-mécanique des Alliés
pour le décryptage



Le décryptage



Marian Adam Rejewski
(1905 – 1980)



Henryk Zygalski (1906-1978)

Ces 2 Polonais ont cassé la première **Enigma** militaire, développé les premiers éléments de la **cryptanalyse** moderne et construit une machine mécanique « **Bomba** » qu'ils ont utilisée pour ce décryptage. Turing améliora la machine et s'en servit au **Bletchley Park** (le centre britannique de l'interception et du décryptage pendant la guerre 1939-1945) pour systématiquement **décoder** les messages de l'aviation nazi

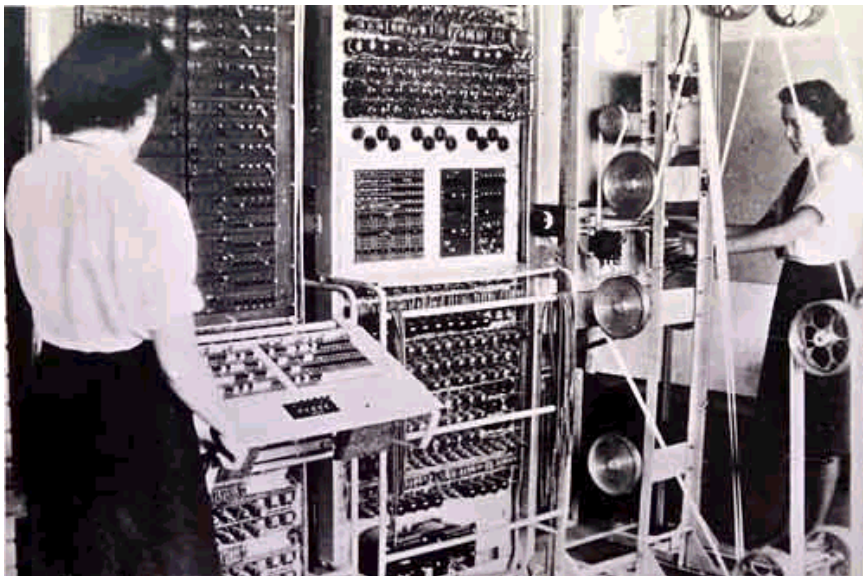
L'ordinateur, enfin

John von Neumann
1903 → 1957

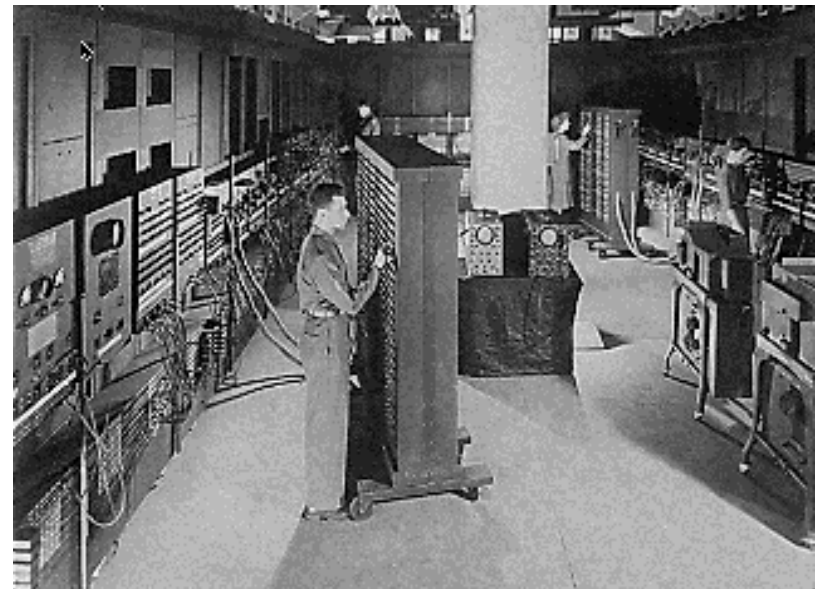


Clarifie le concept de **programme** et des **données**, tout deux stockés dans la **mémoire**.

1943, Colossus



1945, ENIAC



On ne se moque pas

ENIAC:

- un monstre de **30 tonnes**
- **200 kW** de consommation d'énergie nécessitant un **climatisation puissante**
- **19000** lampes électroniques
- **500** relais
- **Des centaines de milliers** de résistances, condensateurs, inducteurs
- carte perforées (données), programmes à la main
- multiplication en **3,5 ms**



10 millions de fois plus puissant...

Électronique

ENIAC = *Electronic Numerical Integrator And Calculator*



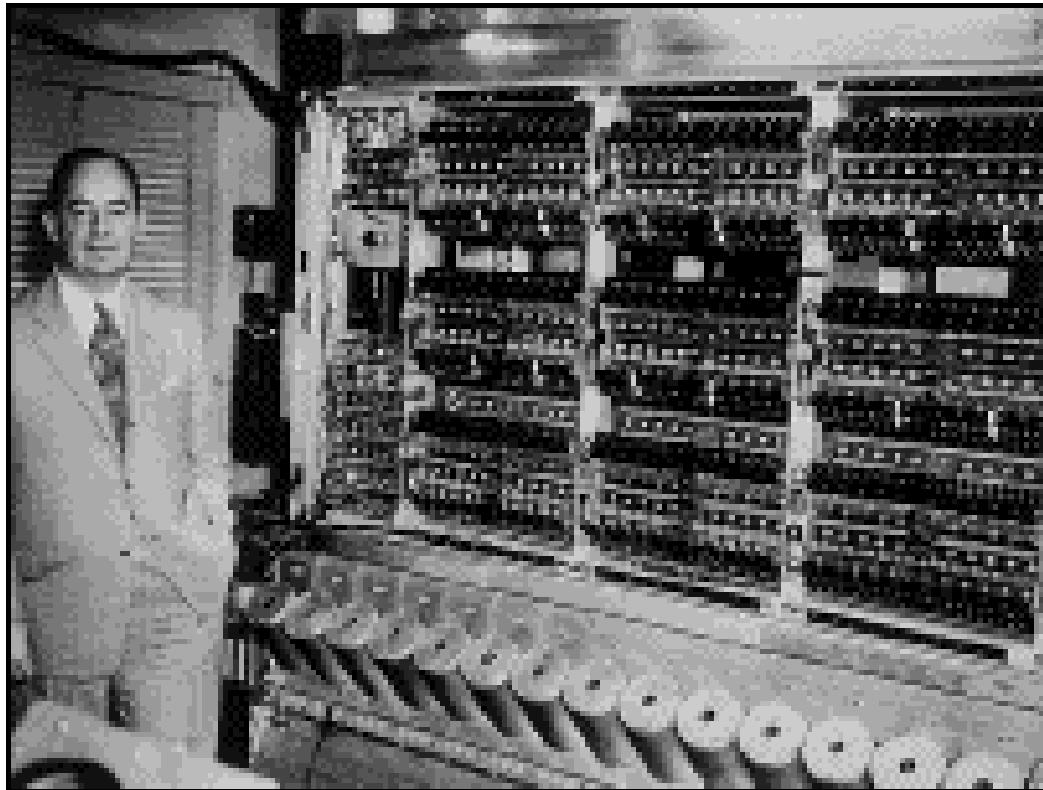
John William **Mauchly** (1907-1980)



John **Eckert** (1919 – 1995)

Première amélioration

- 1945 (mars) : **Eckert** et **Mauchly** signe un contrat pour construire l'**EDVAC** (Electronic Discrete Variable Automatic Computer)
- 1945 (juin) : **Neumann** clarifie le concept de programme stocké dans le rapport du 30 Juin 1945 sur la conception de l'EDVAC . Cela donne le terme « l'**architecture de von Neumann** »

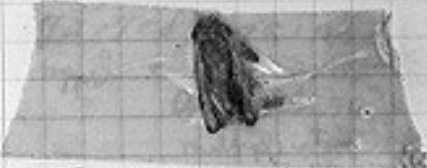


Premier « bug »

92
9/9

0800 Antan started
1000 " stopped - antan ✓
1300 (033) MP-MC 2.130476415
 (033) PRO 2 2.130476415
 convd 2.130676415
Relays 6-2 in 033 failed special speed test
in relay 11,000 test.

1100 Started Cosine Tape (Sine check)
1525 Started Multi-Adder Test.

1545  Relay #70 Panel F
(moth) in relay.

First actual case of bug being found.

1700 Antan started.
1700 closed down.

1.2700 9.037 847 025
9.037 846 995 convd
4.615925059(-2)

Relay 214
Relay 3



Le premier “bug” (vient du monstre mythologique Gallois « bugbear » et déjà utilisé par Thomas Edison vers 1870 pour les pbs mécaniques dans l’industrie) dans le contexte de calcul à l’aide d’un ordinateur. **09/09/1945** : une mite (phalène) a bloqué un relais de Mark II au Naval Weapons Center à Dahlgren, Virginia. Il a été mis dans le rapport (“*First actual case of a bug being found.*”) par l’amiral Grace Murray **Hopper** (1906-1992) qui fut une pionnière dans les compilateurs.

57/71

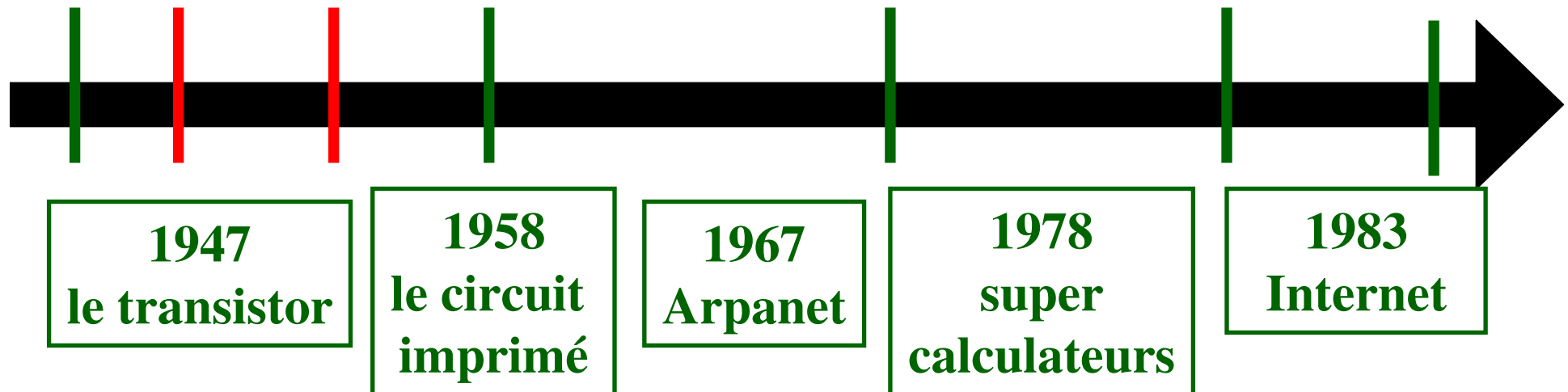
Les temps modernes

Frise chronologique

Théories

1950
complexité
algorithmique

1954
langages
de programmation



Supports physiques

L'électronique

Willam Shockley 1910 → 1989

Walter Brattain 1902 → 1987

John Bardeen 1908 → 1991

Jack Kilby

1923 → 2005



■ **1947** : le premier **transistor** au germanium

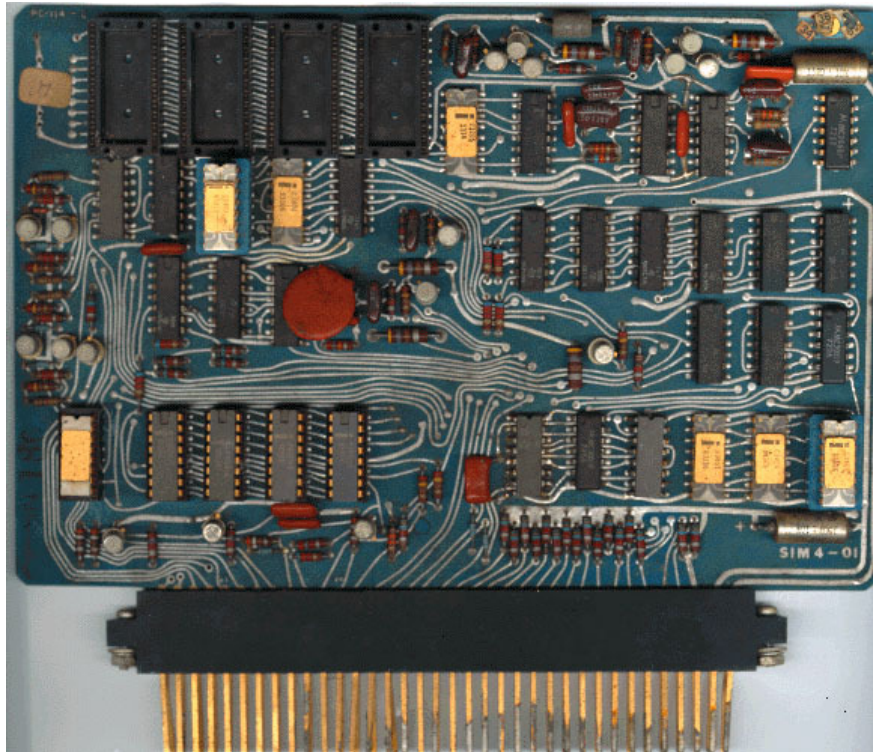
■ **1958** : Texas Instrument ; le premier **circuit intégré** sur germanium

■ **1961** : **Robert Noyce** fabrique le premier circuit imprimé sur **silicium**



Les micro-processeurs

1971 : le premier microprocesseur, Intel 4004

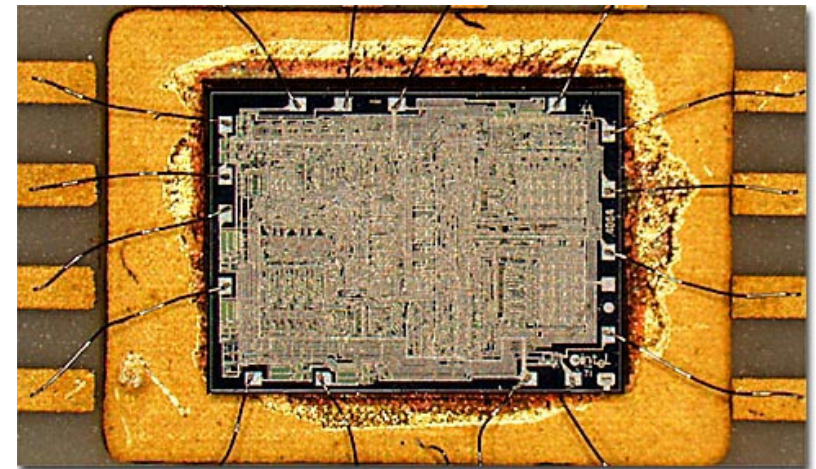


Intel 4004

Ce microprocesseur intègre les opérations logiques, arithmétiques etc., la mémoire et d'autres services

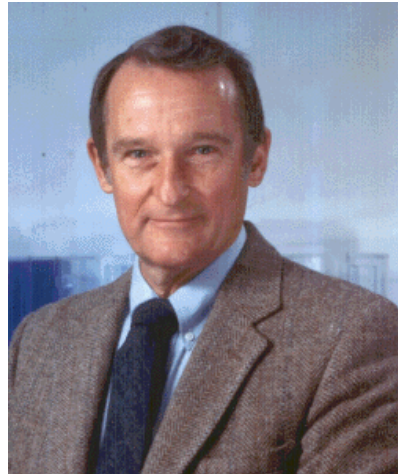


Intel 4040: 740 KHz, 24-pin
– la même vitesse que
Intel 4004, une plus
grande mémoire



La calcul parallèle

Seymour Roger Cray
1925 → 1996



Principe: distribuer les calculs et les données sur différents processeurs ; faire plusieurs choses en même temps.

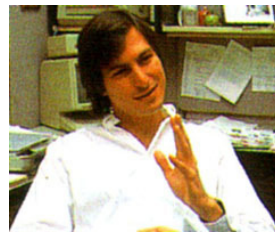
■ **1978** : sortie du premier **super-ordinateur parallèle**, le Cray-1 avec 256 processeurs pour **160 MegaFlops**

■ **2005** : BlueGene/L, IBM, près de 16000 processeurs et **jusqu'à 136 TeraFlops**



Un ordinateur chez vous

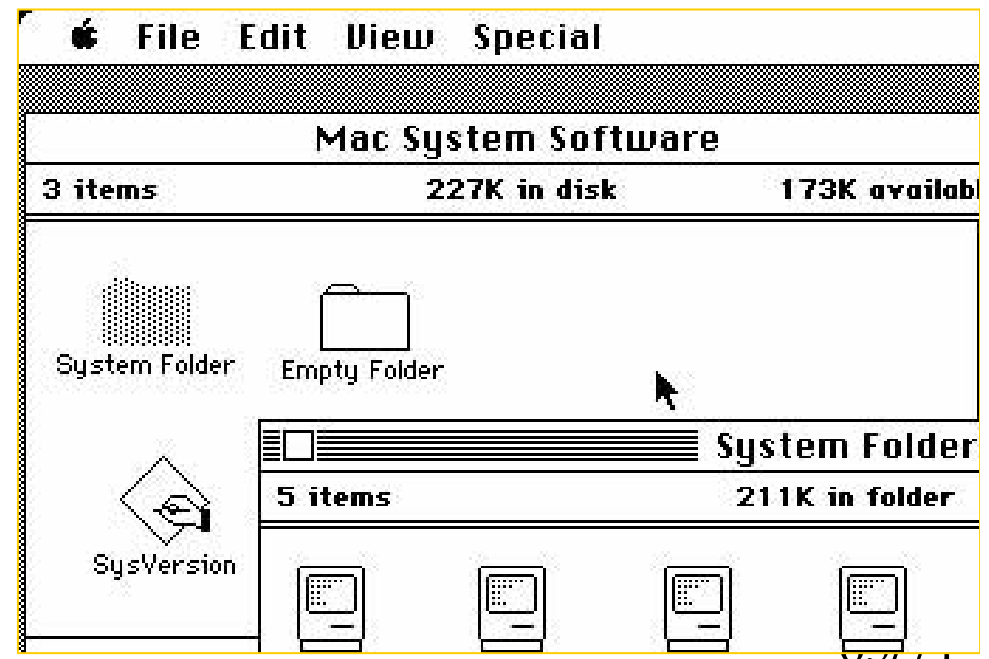
- **1964** : première **souris** par **Doug Engelbart**
- **1973** : le premier **micro-ordinateur** Micral (France).
- **1981** : l'**Osborne 1**, le premier **ordinateur portable** (presque 10 kg), fut mis sur le marché.
- **1984** : Apple (Jobs, Wozniak) commercialisa le Macintosh qui a donné un « standard » de **PC** (personal computer), en particulier d'**interface graphique avec les icônes**.



Steve Jobs



Steve Wozniak



Les réseaux

- **1837** : premiers **télégraphes** avec notamment le morse
- **1896** : premier **télégraphe sans fil**
- **1967** : **Lawrence Robert** publie un article sur le premier réseau mondial, l'**Arpanet**
- **1971** : Envoi du premier **e-mail**
- **1975** : Premiers **réseaux locaux**
- **1983** : Conception du **protocole TCP/IP**, l'Arpanet devient l'**Internet**

ARPA : **A**dvanced **R**esearch **P**rojects **A**gency
Ministère de la défense des Etats-Unis

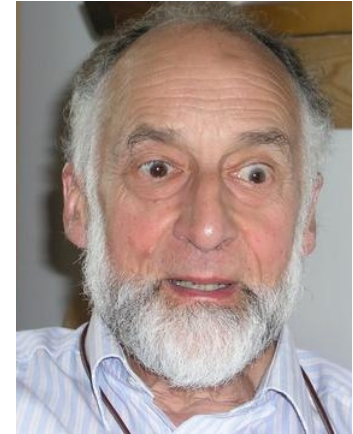
TCP= **T**ransmission **C**ontrol **P**rotocol, **IP** = **I**nternet **P**rotocol.

A • ■■
B ■■■●●
C ■■■■■●
D ■■■●●
E ●
F ●●■■●
G ■■■■■●
H ●●●●
I ●●
J ●■■■■■■
K ■■■●■■
L ●■■■■●
M ■■■■■
N ■■■●
O ■■■■■■
P ●■■■■■●
Q ■■■■■●■■
R ●■■■■●
S ●●●●
T ■■■

U ●●●■■■
V ●●●■■■
W ●■■■■■
X ■■■●●■■
Y ■■■●■■■■
Z ■■■■■●●

1 ●■■■■■■■■
2 ●●■■■■■■
3 ●●●■■■■■
4 ●●●●■■■■
5 ●●●●●■
6 ■■■●●●●
7 ■■■■■●●●
8 ■■■■■■■●●
9 ■■■■■■■■■●
0 ■■■■■■■■■■

Langages de Programmation



John Backus Alan Kay Kristen Nygaard Haskell Curry Robin Milner

■ **1954 : Fortran** (Forma Translator), premier langage de programmation :
Langage impératif de John **Backus**.

■ **1955 : LISP**, langage fonctionnel de John **McCarty**

■ **1958 : Algol**, amélioration de Fortran (Equipe **Backus**)

■ **1967 : Simula**, langage orienté objets de Ole-Johan **Dahl** et Kristen **Nygaard**

■ **1970 : ADA**, premier langage des systèmes embarqués

■ **1975 : ML**, langage fonctionnel basé sur une théorie des types (Haskell **Curry**
1900-1982, Robin Milner, aussi processus concurrents)

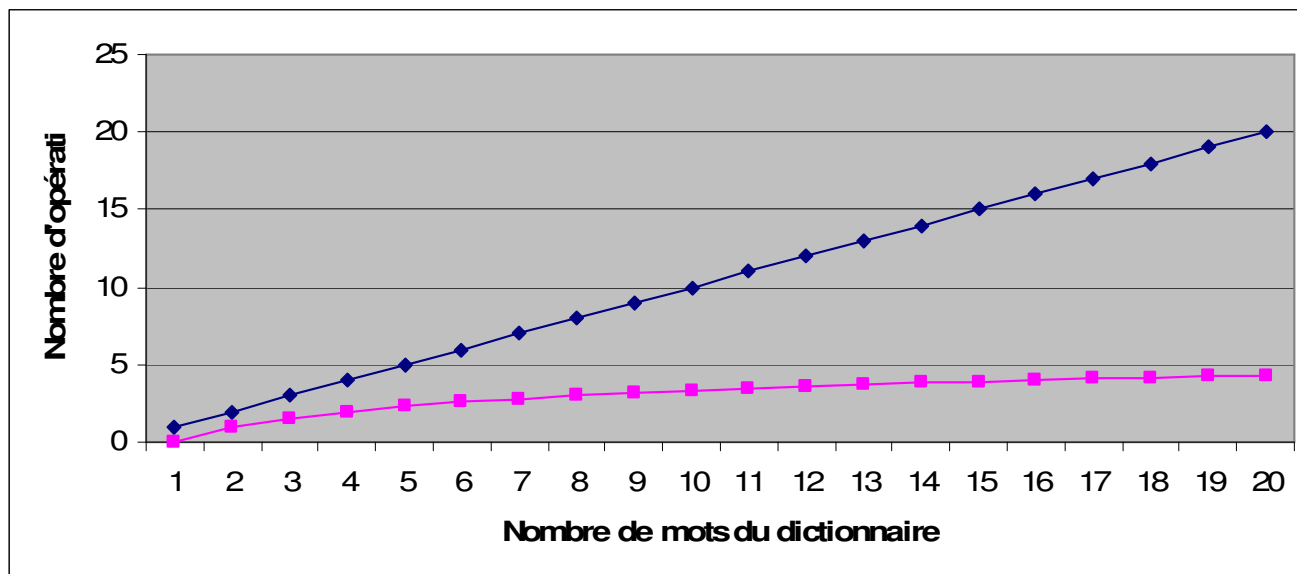
■ **1976 : Smalltalk**, langage orienté objet (Alan **Kay**)

Complexité algorithmique

Donald Knuth



Introduit plus formellement le concept de **complexité algorithmique** = suivant la méthode utilisée un calcul ne se fera pas en un même temps.
Exemple : **rechercher un mot** dans un **dictionnaire**



Recherche linéaire

Recherche logarithmique

Systemes d'exploitations



Dennis Ritchie

**Kenneth
Thompson**

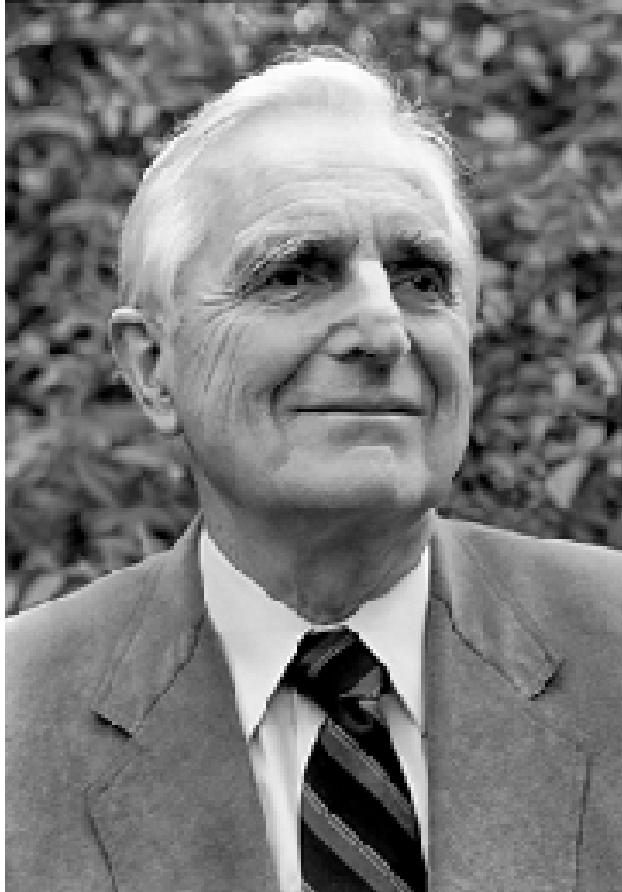
**Linus Benedict
Torvalds**

**Richard
Stallman**

Bill Gates

- **Unix** dans les années 70 (**Ritchie**, **Thompson**); c'est le système d'exploitation (operating system) le plus connu; Encore présent dans certains serveurs d'Internet
- Ancêtre de **GNU/Linux** (1991, **Torvalds**, **Stallman**)
- Bien mieux que **MS-DOS** (1973 et 1981, **Gates**), **Windows** (1988 et 1995, Microsoft)

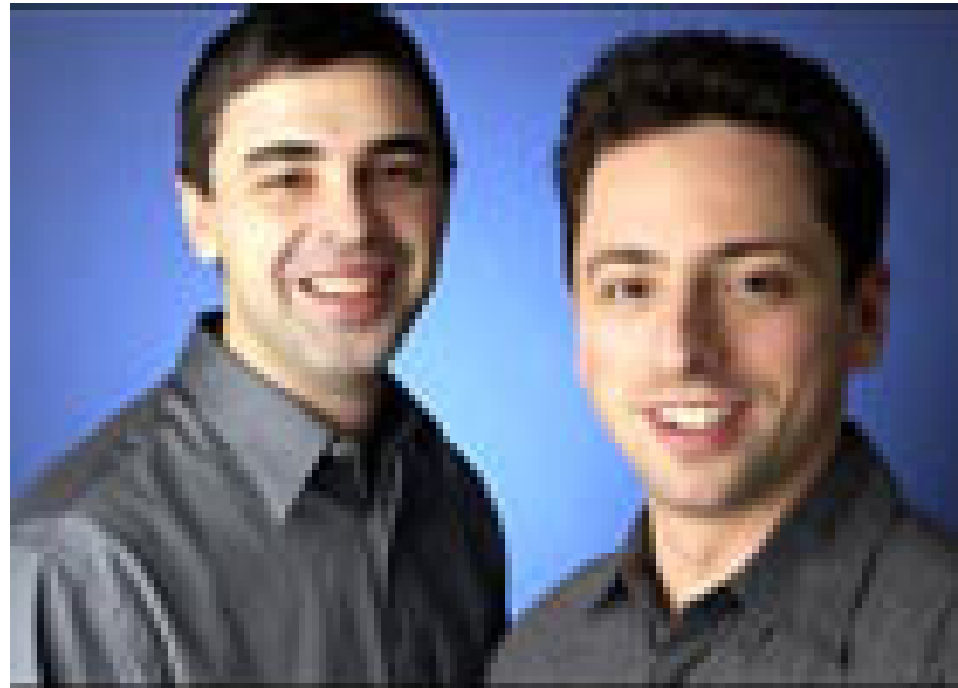
Souris ;-)



- 1964: Doug **Engelbart**. L'utilisation commerciale 20 ans plus tard. Doug Engelbart est un des pionniers de l'Internet
- 1968 : il réalise la première vidéo conférence

Recherche d'informations

Exemple **Google** (Sergy **Brin** & Larry **Page**)

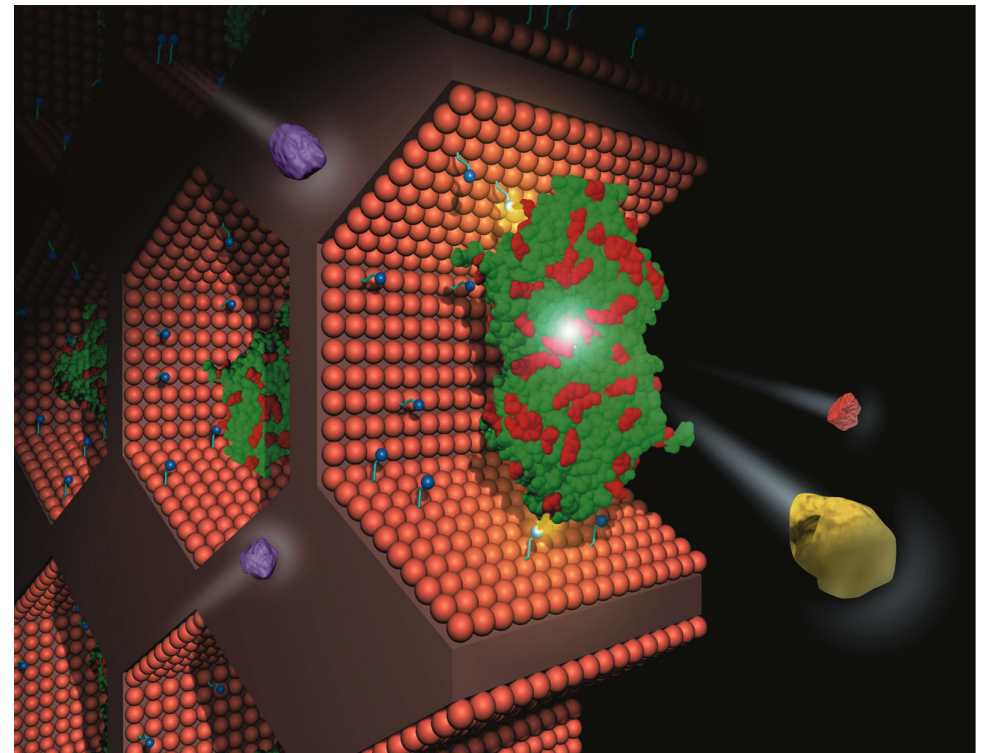


Le mot « Google » a été introduit en 1938 par Milton Sirotta, un neveu de 9 ans du Mathématicien américain Edward Kasner pour nommer le nombre représenté par 1 suivi par cent zéros. Google utilise ce terme pour souligner le but de cette entreprise de faire une quantité immense d'information accessible sur le Web.

Le Futur...

L'informatique d'aujourd'hui est en pleine expansion. On voit un progrès impressionnant dans les applications de l'informatique non traditionnelles :

- bio-informatique
- géologie
- littérature
- aérospatiale
- conception et analyse industrielle
- etc.



Modélisation du comportement d'un enzyme à l'aide d'un super-ordinateur

A la semaine prochaine !