Introduction à l'Informatique Théorique

Master Systèmes Complexes
2009/2010

Cours (20h) : Eric Thierry

TD (10h) : Jonathan Grattage

L’informatique

- Usage courant :
  - Utilisation de logiciels.
  - Développement de logiciels.
  - Technologie.
- Science :
  - Élaboration de connaissances universelles.
  - Raisonnement logique.
  - Observation/expérimentation (dans certains cas).

La science informatique

- Science du calcul (dont traitement de l'information).
- L'informatique théorique : fondements logiques et mathématiques de la science informatique.
- L'informatique à part ça :

  architecture (hardware) réseaux
  systèmes (d'exploitation) sécurité
  langages de prog compilation
  bases de données intelligence artificielle
  interface homme/machine …….
- Computer science / computer engineering

L’informatique théorique

Informatique théo.		Maths & logique
Théorie de la calculabilité		Logique mathématique
Théorie de la complexité		Combinatoire
Théorie des automates	↔	Théorie des langages
Théorie de l’information		Théorie des graphes
Sémantique		Interaction avec presque tous les domaines des maths (algèbre, analyse, probas, …)
Algorithmique (générale puis par domaine)		

Questions fondamentales

- Que veut dire *calculer* ? (modèles de calcul)
- Est-ce que tout est calculable (quitte à disposer d'assez de ressources) ? (calculabilité)
- Quand on peut calculer, de quelles ressources a-t-on effectivement besoin (temps, espace, …) ? (complexité)

Des mots

Turing

λ-calcul

P

Hilbert

Church

Automates

Complétude

Indécidable

Gödel

Babbage

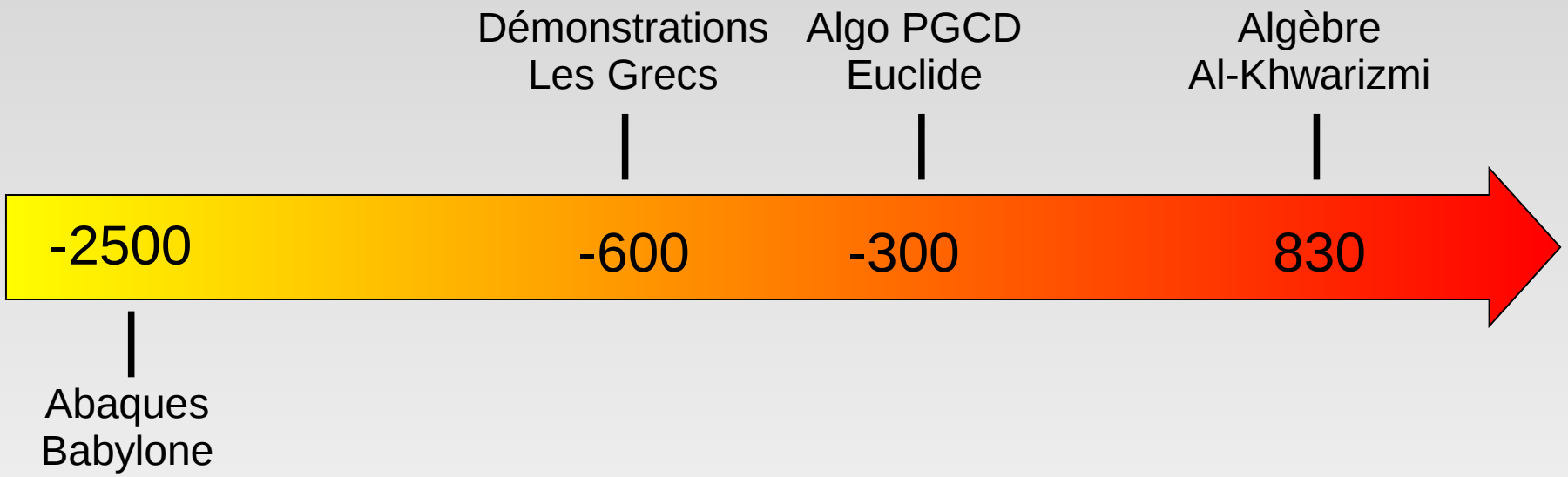
Machine universelle

Récursif primitif

NP

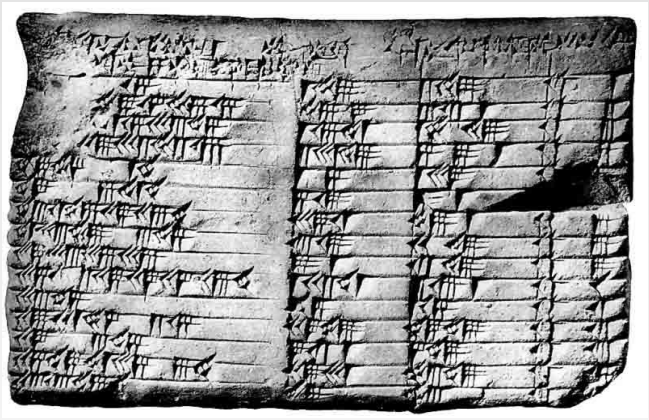
von Neumann

Histoire : il y a longtemps

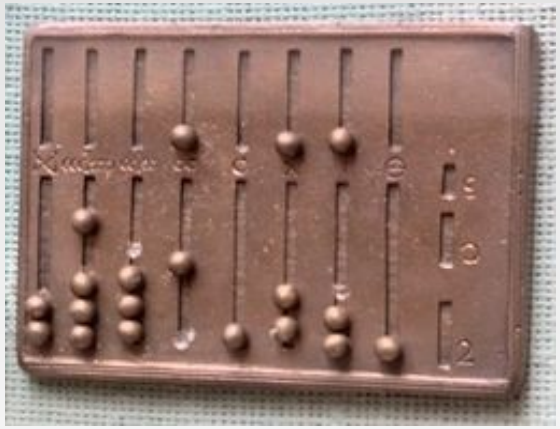


Antiquité

- Abaque : instrument mécanique plan facilitant calcul.
- Babylone -2400, Egypte, Chine, Inde, Grèce, Rome ...



Tablette d'argile
Babylone (-1800)



Abaque romain
(1er siècle)

Grèce antique

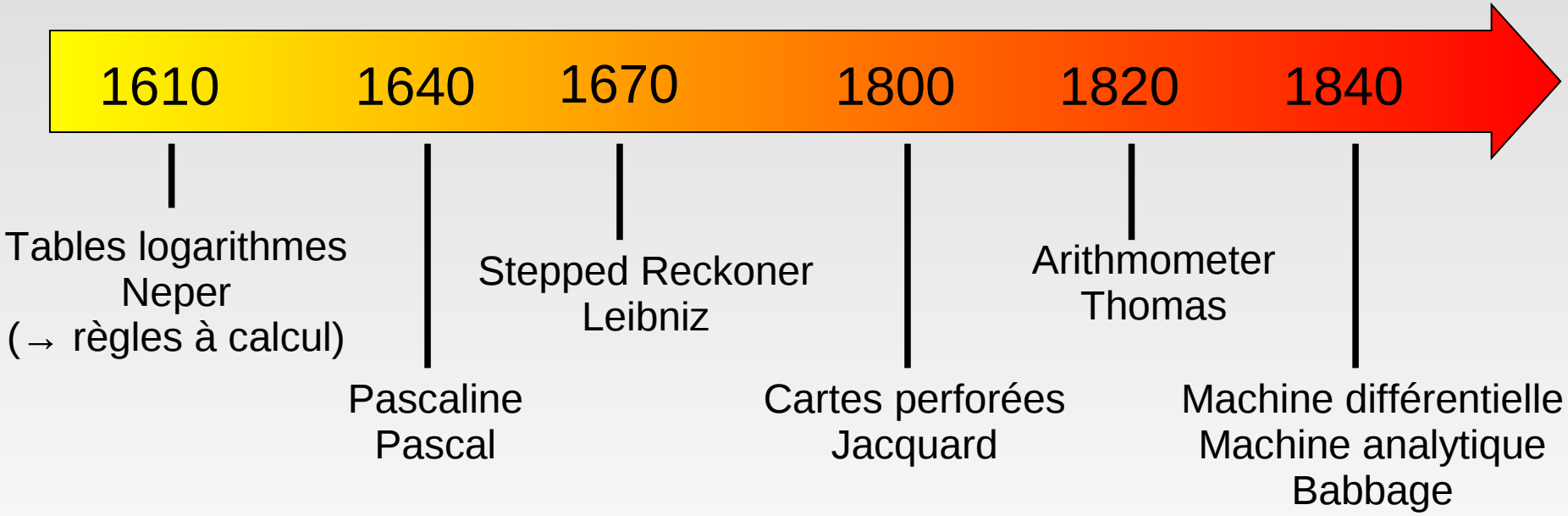
- Approche plus abstraite des mathématiques.
- Mathématiques associées à la philosophie.
- Naissance de la démonstration (Thalès, Pythagore, Hippocrate, Eudoxe, Euclide ...).

Grèce antique

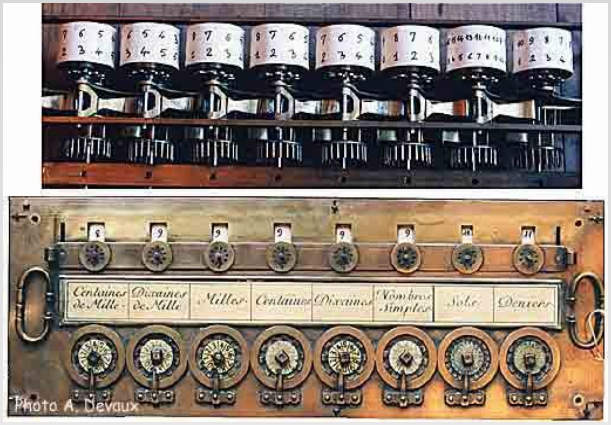
- *Les Eléments* (13 livres) : une synthèse avec traitement axiomatique et systématique en géométrie et arithmétique (déf., axiomes, théo., démo, rigueur).
- Algorithme de calcul du PGCD (Livre 7) : plus ancien algorithme non trivial connu.

Euclide
(-325 - -265)

Histoire : il n’y a pas si longtemps



Les premières calculettes

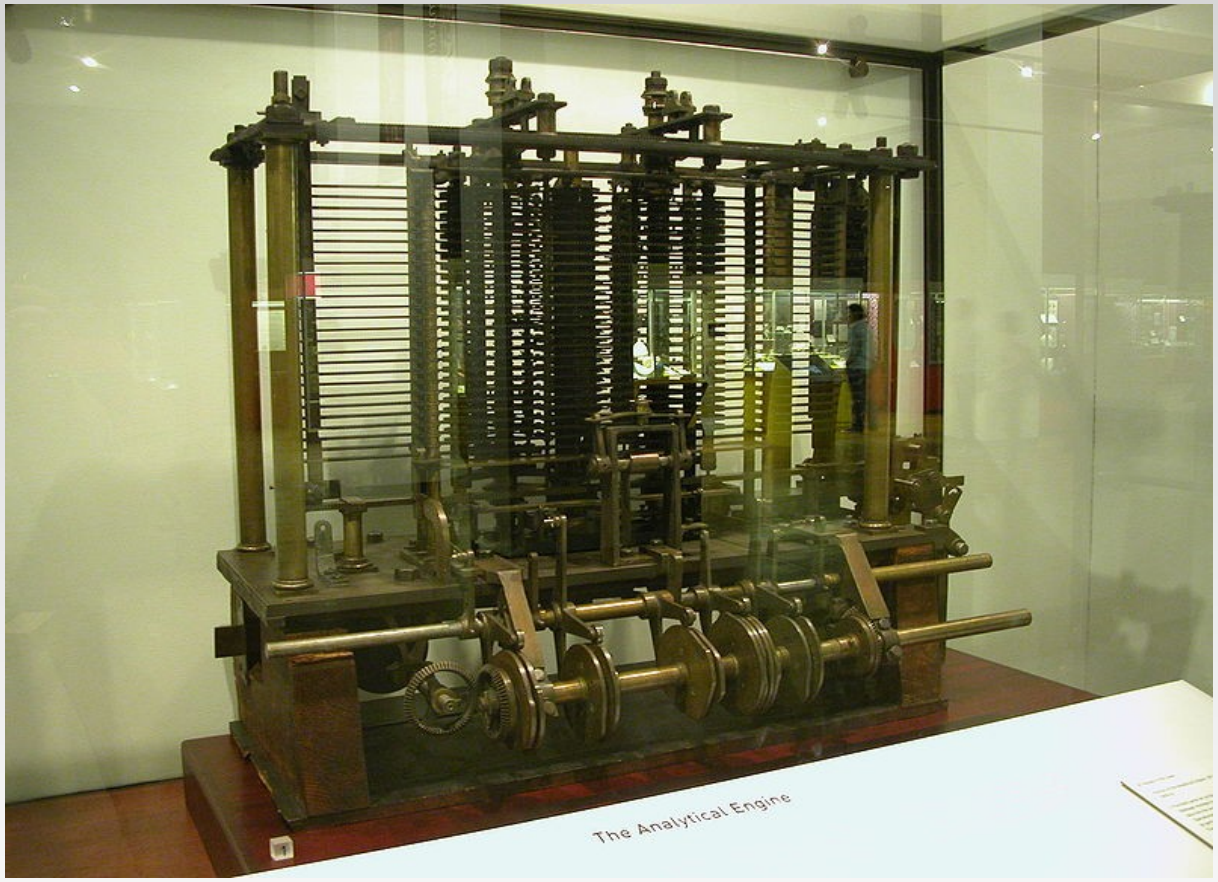


Pascaline
(Pascal,1640)
+,-,(x),(/)

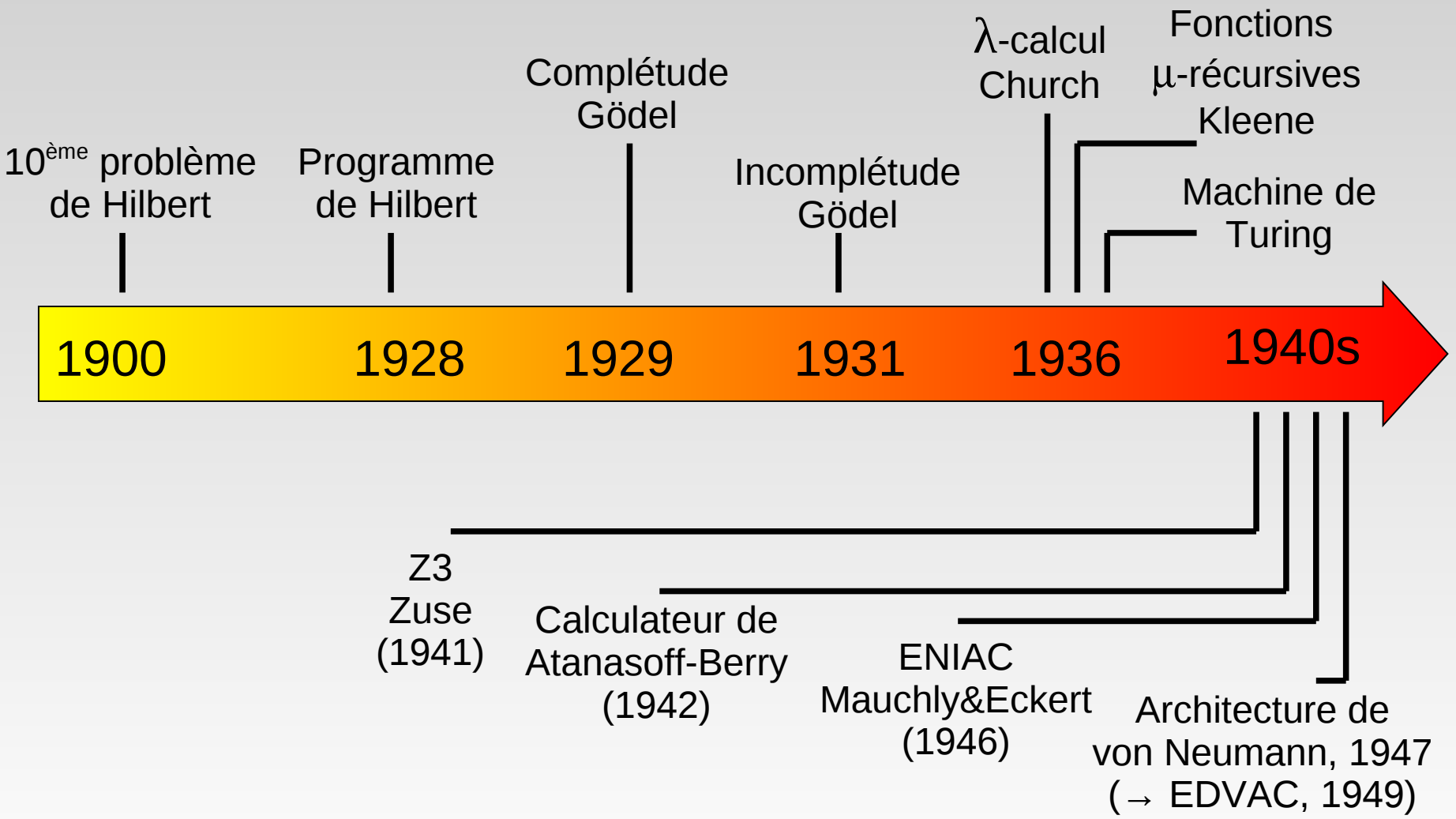
Stepped Reckoner
(Leibniz, 1670)
+,-,(x),(/)

Arithmomètre
(Thomas, 1820)
+,-,x,/

Babbage



Histoire : la naissance



Problèmes de Hilbert

- Au 2ème congrès des mathématiciens (1900), Hilbert présente 23 problèmes.
- 10ème problème : « Trouver un procédé qui peut déterminer par un nombre fini d'opérations si un système d'équation diophantiennes admet une solution ou non ».

Hilbert
(1862-1943)

Programme de Hilbert

- Nouveau congrès (1928) et trois questions fondamentales sur les mathématiques :
  - Complétude ?
  - Cohérence / consistance ?
  - Décidabilité ?

Hilbert
(1862-1943)

Logique mathématique

- Complétude d'une théorie mathématique : tout énoncé valide est démontrable.
- Cohérence d'une théorie mathématique : est-il possible de démontrer un énoncé et sa négation ?
- Décidabilité d'une théorie mathématique : existe-t-il une procédure pour décider si un énoncé est valide ou non ?

Valide / Démontrable

- Ensemble d'énoncés (règles de syntaxes)
- Ensemble d'axiomes
- Enoncé valide : tout modèle satisfiant les axiomes satisfait aussi l'énoncé.
- Enoncé démontrable (pour un système de déduction fixé) : pouvant être obtenue à partir des axiomes avec les règles d'inférence du système (règles de transformations syntaxiques).

De la complétude

- Complétude de la logique du premier ordre, par Gödel (1929).
- Exemples d'énoncés :

$$\exists x \forall y P(x,y) \rightarrow \forall y \exists x P(x,y)$$

$$\exists x \forall y P(x,y) \rightarrow \forall y \exists x P(x,y)$$

Gödel
(1906-1978)

De l’incomplétude

- Incomplétude de l’arithmétique, par Gödel (1931).
- Dans sa démonstration, Gödel utilise une notion de fonctions calculables.

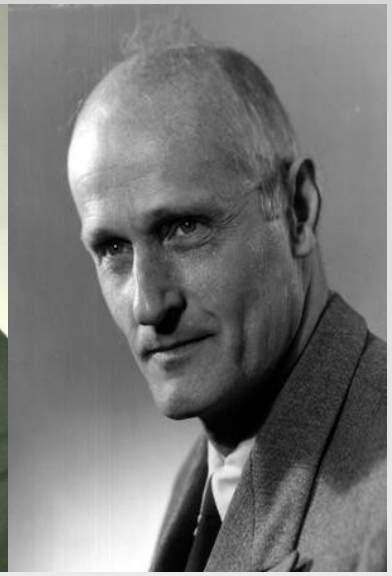
Gödel
(1906-1978)

Calculabilité

- Church et Kleene introduisent des définitions équivalentes d'une classe générale de fonctions calculables.
- Fonctions récursives :

f(0,x,y)=x
f(n+1,x,y)=f(n,x+y,y+2)
f(n,0,1) ?

Church
(1903-1995)



Kleene
(1909-1994)

Calculabilité

- Machine abstraite :

Turing
(1912-1954)

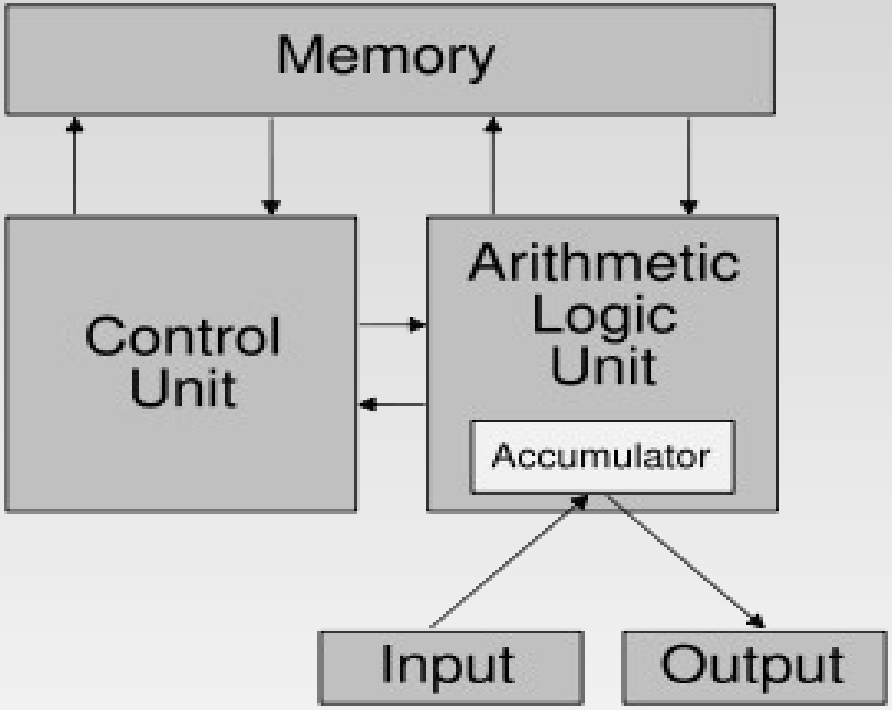
- Indécidabilité de l’arrêt des machines de Turing.
- Indécidabilité de la logique du premier ordre.

Thèse de Church (1943)

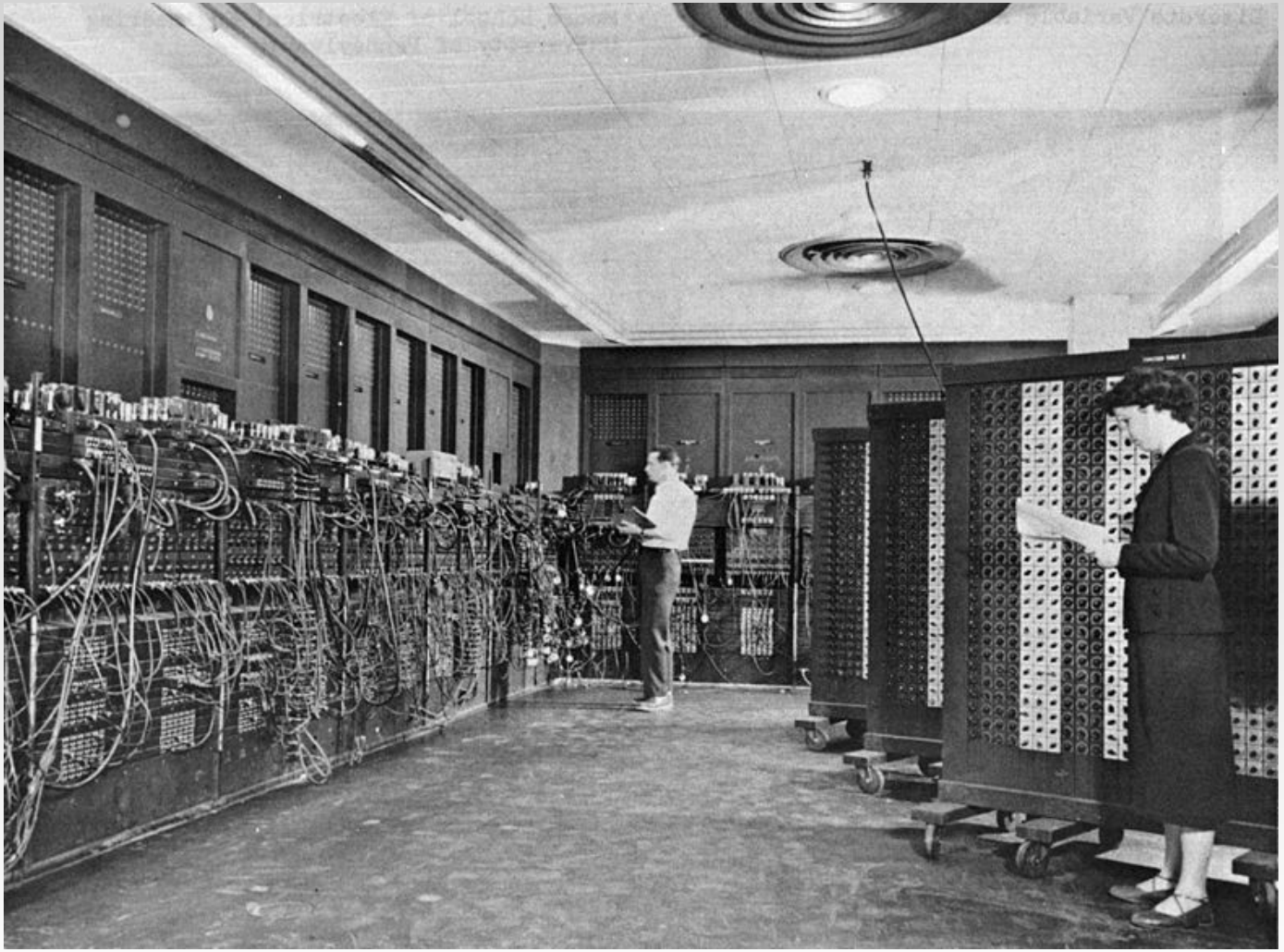
- Les notions de fonctions calculables qui ont été formalisées sont :
  - équivalentes (affirmation démontrée mathématiquement)
  - exactement la formalisation de la notion intuitive de calcul / procédure / algorithme (philosophie).

Church
(1903-1995)

von Neumann architecture



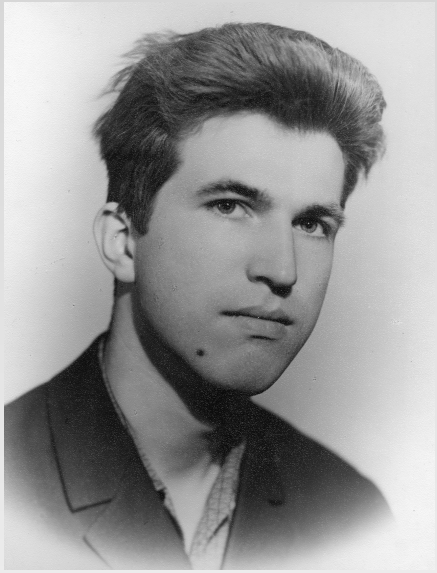
ENIAC



Histoire : les temps modernes

$10^{ème}$ problème de Hilbert

- Matiyasevitch démontre l'indécidabilité du $10^{ème}$ problème de Hilbert (1970).



Matiyasevitch
(1947-)

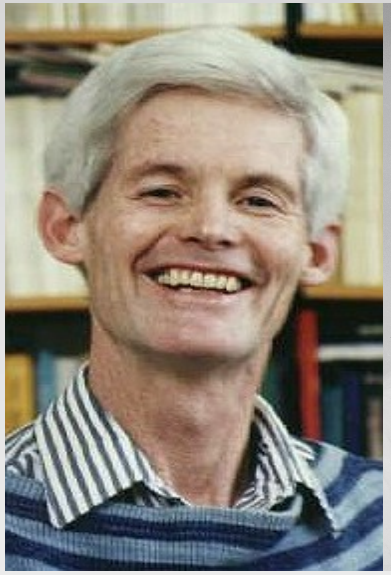
Complexité

- Problèmes polynomiaux (*P*) : problèmes pour lesquels on peut trouver une solution en temps polynomial, càd borné par n^p où :
  - *n* est la taille des données,
  - *p* est un exposant fixé (ne dépendant que du problème).
- Problèmes *NP* : problèmes pour lesquels on peut vérifier en temps polynomial si une solution candidate est valide.

Complexité

- Conjecture introduite simultanément par Cook et Levin (1970): P ≠ NP ?
- Millenium problem (2000)

$ 1000000



Cook
(1939-)

Levin
(1948-)