Comment les mathématiciens ont inventé l'ordinateur

Denis Kuperberg

Journés JTM
01/07/2015
Toulouse

Introduction

Algorithme :
Suite d'instructions à effectuer pour résoudre un problème.

Exemples :

- Poser une addition, multiplication,...
- Donner des directions
- Recette de cuisine

Introduction

Algorithme :
Suite d'instructions à effectuer pour résoudre un problème.

Exemples :

- Poser une addition, multiplication,...
- Donner des directions
- Recette de cuisine

- *Arithmétique* : Science des nombres
- *Géométrie* : Science des formes
- *Informatique* : Science des algorithmes

Antiquité

-300 : **Euclide** algorithme du plus grand diviseur commun :

$$68 - 24 = 44$$
$$44 - 24 = 20$$
$$24 - 20 = 4$$

Antiquité

-300 : **Euclide** algorithme du plus grand diviseur commun :

$$68 - 24 = 44$$
$$44 - 24 = 20$$
$$24 - 20 = 4$$

≈-100 : **Machine d'Anticythère**

- mouvement des planètes
- prévoit les éclipses
- date des Jeux Olympiques

Mathématiques arabes

825 : **Al-Khwarizmi** à Bagdad :

- Nombre décimaux (indiens)
- Al-gorithme
- “inventeur” de l’algèbre
- Résout les équations du type $x^2 - 5x + 12 = 0$ par un algorithme

Nouvelles machines

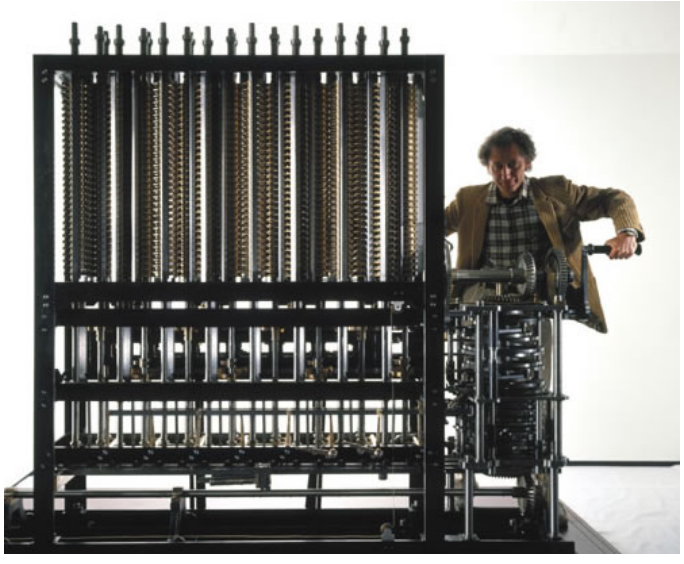
1642 : **Blaise Pascal** : Pascaline, calculatrice pour additions et soustractions.

Nouvelles machines

1642 : **Blaise Pascal** : Pascaline, calculatrice pour additions et soustractions.

1837 : machine de **Charles Babbage**

- Machine théorique
- Fonctions mathématiques complexes
- “Programmable”



1842 : **Ada Lovelace**

- Première programmeuse
- Vision : machine $\rightarrow$ musique
- Langage Ada en son honneur

Les problèmes du siècle

1900 : **23** problèmes de **Hilbert** pour les mathématiciens du siècle

- $2^{ème}$ *problème* : preuve de la cohérence de l'arithmétique ? 2=1 ?
- $10^{ème}$ *problème* : algorithme pour résoudre les équations entières ?

Exemple : $x^2 + 3y + 5 = 0$ et $x - 4y^3 = 7$?

Les problèmes du siècle

1900 : **23** problèmes de **Hilbert** pour les mathématiciens du siècle

- $2^{ème}$ *problème* : preuve de la cohérence de l'arithmétique ? 2=1 ?
- $10^{ème}$ *problème* : algorithme pour résoudre les équations entières ?

Exemple : $x^2 + 3y + 5 = 0$ et $x - 4y^3 = 7$?

Essayer toutes les possibilités ?

Les problèmes du siècle

1900 : **23** problèmes de **Hilbert** pour les mathématiciens du siècle

- $2^{ème}$ *problème* : preuve de la cohérence de l'arithmétique ? 2=1 ?
- $10^{ème}$ *problème* : algorithme pour résoudre les équations entières ?

Exemple : $x^2 + 3y + 5 = 0$ et $x - 4y^3 = 7$?

Essayer toutes les possibilités ?

OK s'il existe une solution,
Infini s'il n'y en a pas.

Les problèmes du siècle

1900 : **23** problèmes de **Hilbert** pour les mathématiciens du siècle

- $2^{ème}$ *problème* : preuve de la cohérence de l'arithmétique ? 2=1 ?
- $10^{ème}$ *problème* : algorithme pour résoudre les équations entières ?

Exemple : $x^2 + 3y + 5 = 0$ et $x - 4y^3 = 7$?

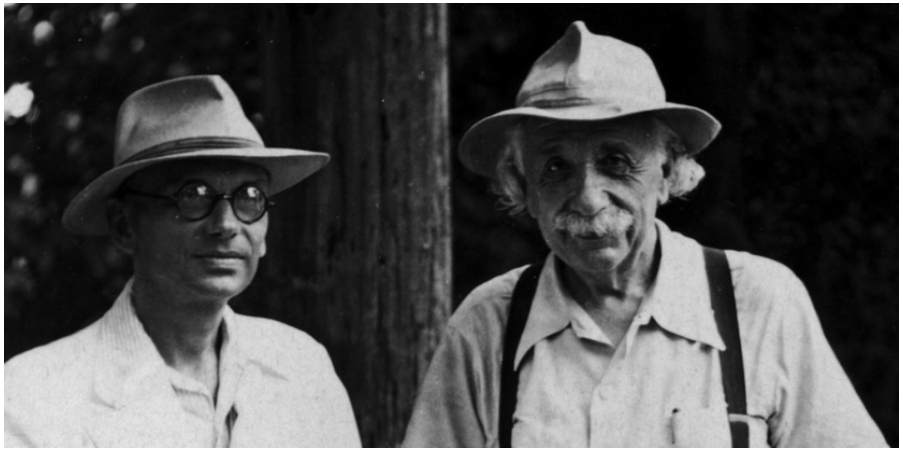
Essayer toutes les possibilités ?

OK s'il existe une solution,
Infini s'il n'y en a pas.

Les 23 problèmes aujourd'hui :
10 résolus, 7 partiellement, 3 non résolus, 3 trop vagues.

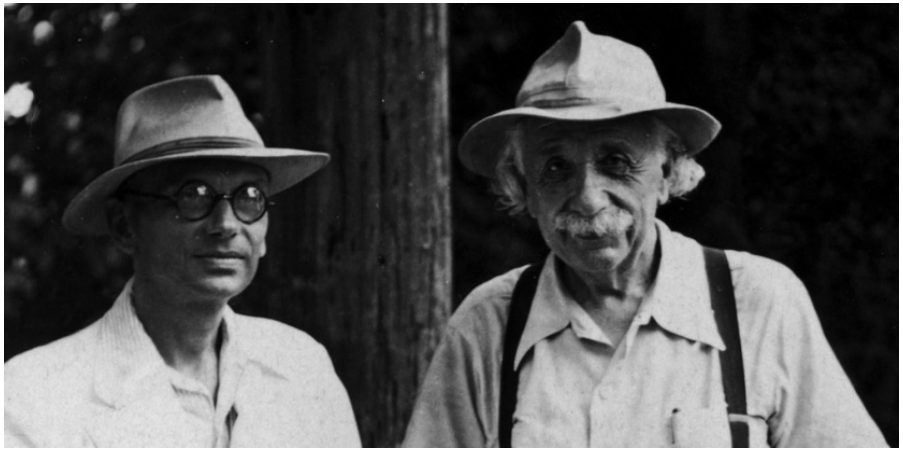
L'incomplétude de Gödel

1931 : **Kurt Gödel** : les maths sont *incomplètes* (et le resteront).



L'incomplétude de Gödel

1931 : **Kurt Gödel** : les maths sont *incomplètes* (et le resteront).

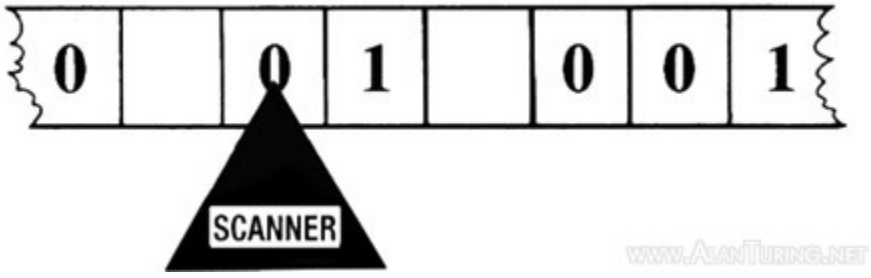


Idées :

- On peut représenter les preuves par des nombres
- Vérifier une preuve $\Leftrightarrow$ Calculer avec $+$ et $\times$
- Equation "Je suis improuvable" $\rightarrow$ vraie mais improuvable
- Equation "L'arithmétique est cohérente" vraie et improuvable $\rightarrow$ $2^{\text{ème}}$ problème résolu.

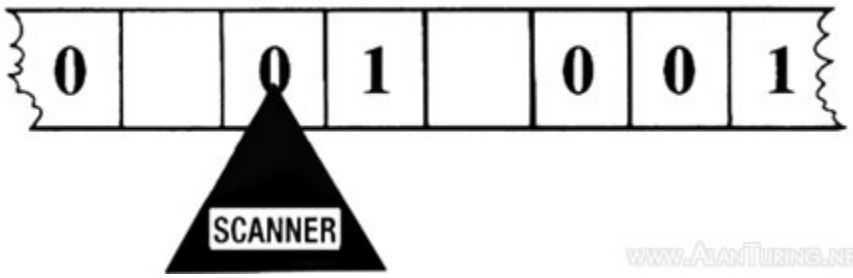
Turing et sa machine

Question : Qu'est-ce qu'un algorithme ?
1936 : Humain+papier,crayon $\rightarrow$ Machine de **Turing**.

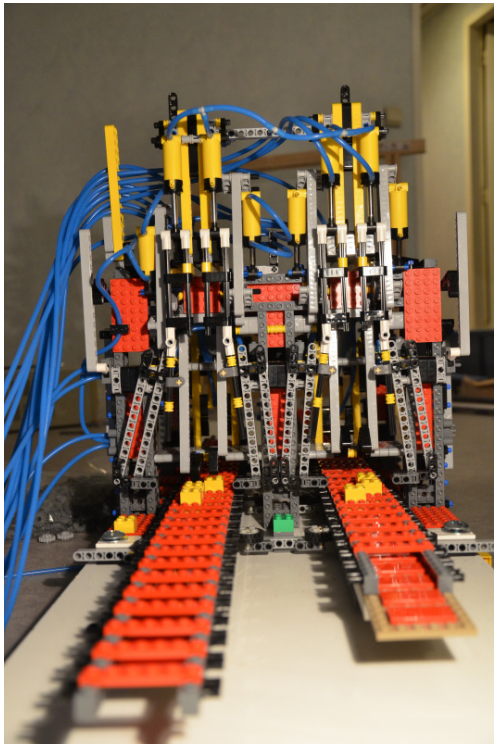


Turing et sa machine

Question : Qu'est-ce qu'un algorithme ?
1936 : Humain+papier,crayon $\rightarrow$ Machine de **Turing**.



Machine théorique :
le scanner a une limite de mémoire, mais la bande est infinie.



Exemple de programme

Question : Suite de 0 et 1 est la même en miroir ?

Cases : Blanc (B), $0, 1$; Etats du scanner : p, d_0, d_1, g, r_0, r_1

Etat	Case	Ecriture	Direction	Nouvel état
p	0	B	$\rightarrow$	d_1
p	1	B	$\rightarrow$	d_1
p	B		Accepte	
d_0	0	0	$\rightarrow$	d_0
d_0	1	1	$\rightarrow$	d_0
d_0	B	B	$\leftarrow$	r_0
d_1	0	0	$\rightarrow$	d_1
d_1	1	1	$\rightarrow$	d_1
d_1	B	B	$\leftarrow$	r_1
g	0	0	$\leftarrow$	g
g	1	1	$\leftarrow$	g
g	B	B	$\rightarrow$	p
r_0	0	B	$\leftarrow$	g
r_0	1		Refuse	
r_0	B		Accepte	
r_1	0		Refuse	
r_1	1	B	$\leftarrow$	g
r_1	B		Accepte	

Résultats de Turing sur la machine

- Peut faire tous les calculs et algorithmes possibles
- On peut encoder la table d'une machine en $0, 1$
- Machine universelle : simule toutes les autres
- Certaines choses ne sont pas calculables !

Exemples :

- Nombre pair ?
- Pixel du centre est rouge ?
- Trier des mots par ordre alphabétique

Est-ce que la machine encodée va s'arrêter ?

Résultats de Turing sur la machine

- Peut faire tous les calculs et algorithmes possibles
- On peut encoder la table d'une machine en $0, 1$
- Machine universelle : simule toutes les autres
- Certaines choses ne sont pas calculables !

Exemples :

- Nombre pair ?
- Pixel du centre est rouge ?
- Trier des mots par ordre alphabétique

Est-ce que la machine encodée va s'arrêter ? IMPOSSIBLE

Résultats de Turing sur la machine

- Peut faire tous les calculs et algorithmes possibles
- On peut encoder la table d'une machine en $0, 1$
- Machine universelle : simule toutes les autres
- Certaines choses ne sont pas calculables !

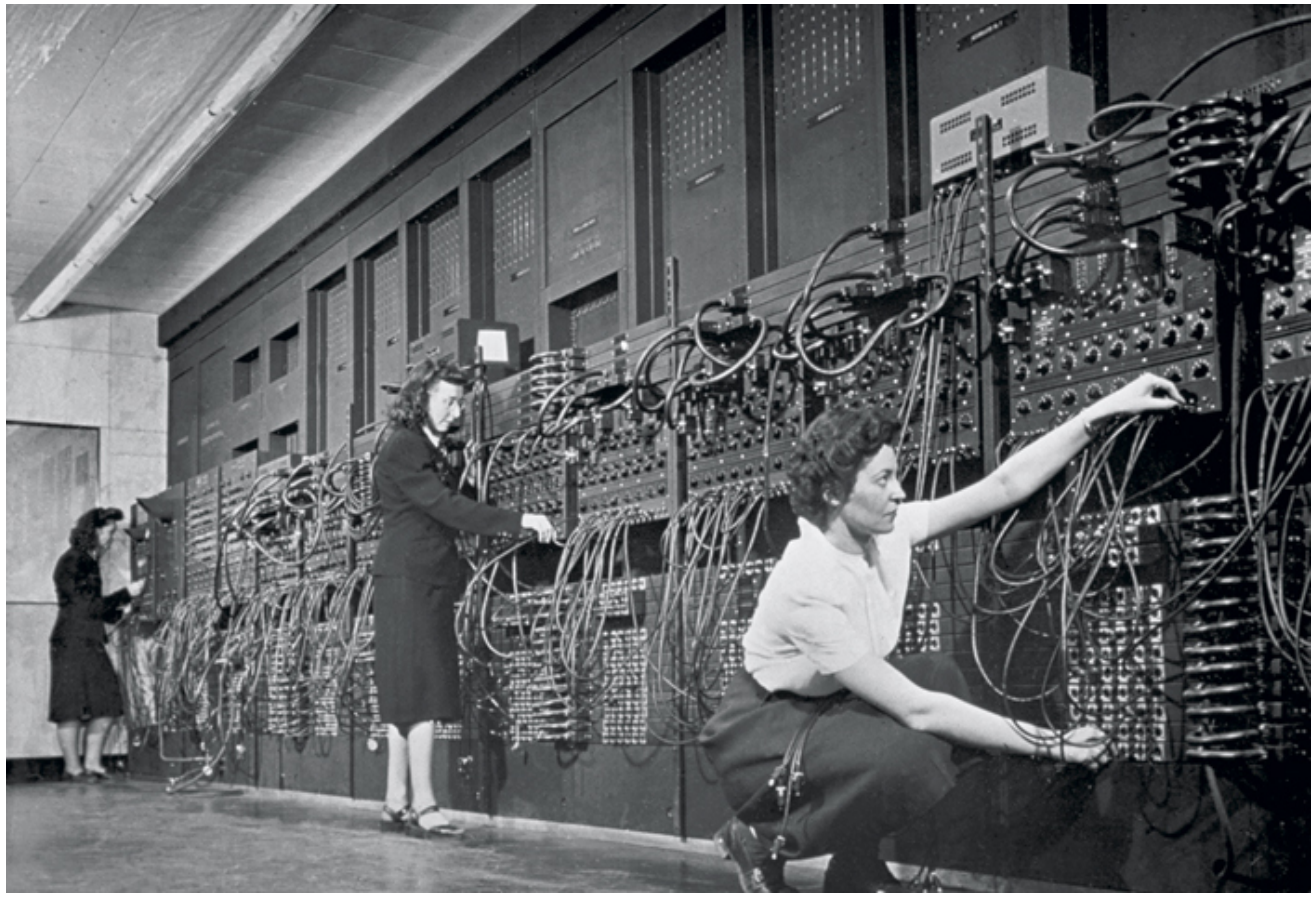
Exemples :

- Nombre pair ?
- Pixel du centre est rouge ?
- Trier des mots par ordre alphabétique

Est-ce que la machine encodée va s'arrêter ? IMPOSSIBLE

1940 : grâce à une autre machine, Turing décrypte le code Enigma des nazis, et aide les Alliés à gagner la guerre.
Il est aidé de linguistes, mathématiciens, joueurs de mots croisés, joueurs d'échecs,...

1946 : ENIAC : Premier ordinateur générique Turing-complet, programmé par 6 femmes



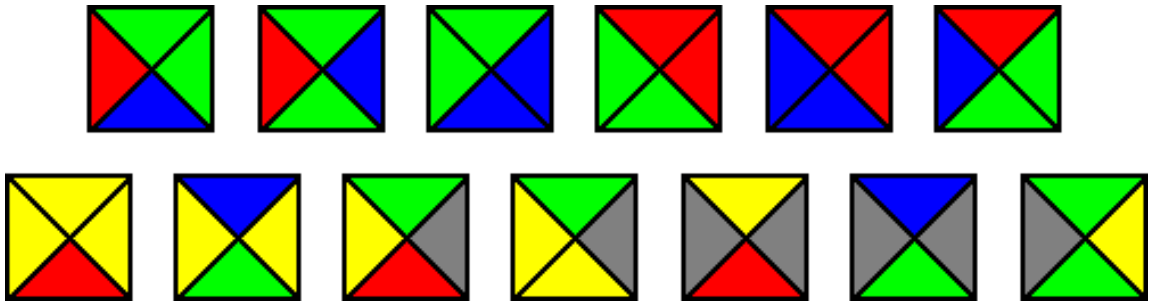
Recherches récentes

1970 : **Matiyasevich** : NON au 10e probleme de Hilbert :
Résoudre une équation $\Rightarrow$ prédire si une machine de Turing va s'arrêter.

Recherches récentes

1970 : **Matiyasevich** : NON au 10e probleme de Hilbert :
Résoudre une équation $\Rightarrow$ prédire si une machine de Turing va s'arrêter.

Autre exemple de problème impossible : tuiles de **Wang** :



Question Peut-on faire un puzzle aussi grand qu'on veut ?

Aucun algorithme n'y répond !

NP-complétude

2000 : 7 problèmes, à 1 million de dollars chacun (1 résolu).

Parmi eux, "$P = NP$?", sur la vitesse des algorithmes :
Les problèmes faciles à vérifier sont-ils faciles à résoudre ?

NP-complétude

2000 : 7 problèmes, à 1 million de dollars chacun (1 résolu).

Parmi eux, "$P = NP$?", sur la vitesse des algorithmes :
Les problèmes faciles à vérifier sont-ils faciles à résoudre ?

Problèmes NP-complets :

- Visiter 30 villes en moins de 1000km ?
- Manger au restaurant pour exactement $20c$?
- Caser toutes les matières dans l'emploi du temps ?
- Et des milliers d'autres, tous équivalents.

Peut-on faire mieux qu'essayer toutes les solutions ?

Si oui pour un, oui pour tous !