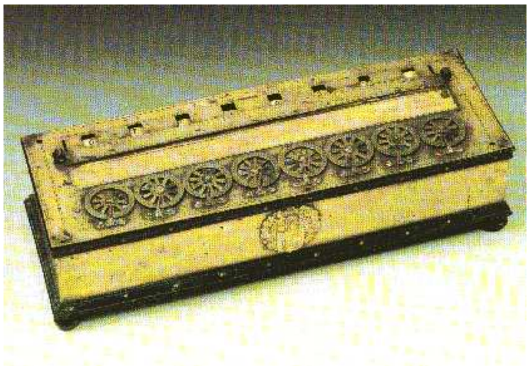
Jours de Sciences (mars 2000)
Les Mureaux

Le temps en mathématiques et en informatique


Cyril.Banderier@inria.fr

Des automates aux ordinateurs

Les horloges de plus en plus performantes et les automates sont bien sûr les ancêtres de nos modernes ordinateurs.



La machine de Pascal

Boulier, abaque (calculs)
Pascaline (1642)
Longitude/latitude
Orgue de Barberi (1700)
Métier Jacquard (1790)
Machine de Babbage (1837)
PC (1984)

Machines à “compter” ou à “ordonner” ?
computer / ordinateur
computer science / informatique

Temps & harmonie

Pythagore (-569, -475)

"Tout est harmonie. Tout est rapport."
(musique/géométrie/nombres)

Scandale : la diagonale du carré n'est pas un "rapport" = une "fraction".

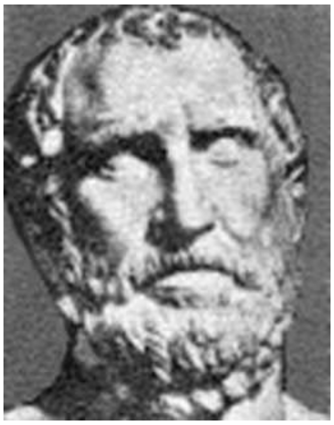
Théorème : $\sqrt{2}$ *est irrationnel.*
Preuve (Euclide, "reductio ad adsurbum"):
On suppose p/q irréductible

$$\sqrt{2} = p/q \Longrightarrow 2 = p^2/q^2$$

$$\Longrightarrow 2q^2 = p^2 \Longrightarrow 2q^2 = (2p')^2 \Longrightarrow q^2 = 2p'^2$$

donc q était aussi un nombre pair
impossible car p/q était irréductible
donc la supposition était fausse. CQFD!

Un temps infiniment divisible ?



Zénon d'Élée (-490,-425)

Paradoxes de Zénon d'Elée :
"Achille ne rattrape pas la tortue."
"La flèche n'atteindra pas son but."
Il reste toujours la moitié du temps, de la distance, (donc temps infini ou distance infinie à parcourir)
$\Rightarrow$ Zénon : Le temps n'est pas divisible à l'infini
$\Rightarrow$ Nous : mauvaise compréhension de la notion convergence

$$1/2 + 1/4 + 1/8 + 1/16 + 1/32 + 1/64 + \cdots = 1$$

temps discret /temps continu...

Newton (1643-1727) et Leibniz (1646-1716)

Querelle des infinitésimaux,
naissance du calcul différentiel
Newton : tangente
Leibniz : analyse non standard
Cauchy : rigoureux "continuité"
$\forall\, \epsilon \exists \delta$ t.q. $|x-1| \leq \delta \Rightarrow |f(x)-(f(1)| < \epsilon$

Algèbre (al jabr) = science des égalités
Analyse = science des inégalités

Dieudonné : *"Majorer, minorer, approcher"*
précision (calculatrice / calcul formel)
17 millions de décimales de π (Ramanujan)

$$\pi = \frac{9801}{\sqrt{8}} \sum_{n=0}^{\infty} \frac{(4n)!(1103+26390n)}{n!^4 396^{4n}}^{-1}$$

Résoudre un problème millénaire et mourir en duel

Niels Abel (1802-1829) et Évariste Galois (1811-1832)

résoudre $ax + b = 0 \Longrightarrow x = -b/a$

$ax^2 + bx + c = 0 \Longrightarrow x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

$ax^3 + bx^2 + cx + d = 0 \Longrightarrow$ Cardan 1539

$ax^4 + bx^3 + cx^2 + dx + = 0 \Longrightarrow$ Ferrari 1540

Théorème : (Galois, 1832)

"Pas de formule pour équations de degré ≥ 5."

symétries dans solutions $\rightarrow$ théorie des groupes

Il existe des nombres qui ne sont solutions d'aucune équation (nombres "transcendants", ex. : π, donc quadrature du cercle impossible).

La quatrième dimension et même plus

• D'Alembert (Encyclopédie, 1754): "Un ami de ma connaissance conçoit [...]"
4ème dimension = le temps

• Chaque révolution en physique = différente conception de *l'espace-temps* :
Aristote (-384,-322)
Galilée (1564-1542)
Newton (1643-1727)
Minkowski (1964-1909)
Einstein (1879-1955)

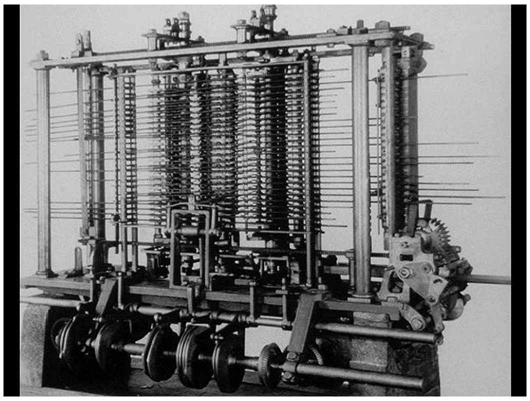
• mathématiques = dégager des *structures*

Ensemble	on gagne	on perd
N	successeur	
Z	opposé	minimum
Q	fractions	successeur
R	convergence	dénombrable
C	toute éq. a solution	ordre
H	aspect quantique	commutativé

Théorie de la complexité

Étude du temps mis par un programme

algorithme : Al-Khwarizmi (780-850)



La machine de Babbage

Complexité = énergie dépensée
= nb de tours de manivelle

analyse d'algorithmes (moyenne, pire des cas)

échecs : Kasparov KO par brute-force
(arbre de possibilité, critère, élagage)
jeu de go : l'ordi est nul.
Intelligence artificielle (test de Turing)

difficile (exponentiel : voyageur de commerce, emploi du temps, sac-à-dos)
facile (polynomial : division, trier)

déterministe // aléatoire

Conjecture de Syracuse :
si n pair, divise par 2, sinon $3n + 1$

$$3 \rightarrow 10 \rightarrow 5 \rightarrow 16 \rightarrow 8 \rightarrow 4 \rightarrow 2 \rightarrow 1$$

"On finit toujours par tomber sur 1"

Il n'existe pas de moyen "universel" pour dire si un programme va s'arrêter ou pas.

green Cryptographie

$\kappa\rho\upsilon\pi\tau o\sigma$ (secret) + $\gamma\rho\alpha\phi\epsilon\iota\nu$ (écrire) = science des codes secrets.

Jules César : décale alphabet de 3 crans (bêta !)

L'armée, moteur d'avancées scientifiques :
→ mécanique pour balistique
→ formation des gradés (Polytechnique 1794)
→ communication à distance (fabriquer un code secret)
→ simulation temps réel (Flight simulator)
→ réseau Internet (Arpanet USA 1969)
→ "casser" les codes secrets (premiers ordinateurs : Enigma)

Nombres premiers $= 2, 3, 5, 7, 11, 13, 17, 19...$

Théorème (Euclide) :

" Il existe infinité de nombres premiers"

Preuve: Supposons qu'il n'y en ait que 3, alors $p_1 p_2 p_3 + 1$ serait premier, d'où la contradiction! QED

codes secrets *basés sur nombres premiers*

(car *factorisation* en nombres premiers prend beaucoup de temps)

facile : calculer 29×71

difficile : factoriser 2059

très difficile : factoriser

$2^{2^9} + 1 =$ 1340780792994259709957402499820584612747936582059

2393377723561443721764030073546976801874298166903427690031

858186486050853753882811946569946433649006084097

Système à clef publique : RSA (1977)

$\rightarrow$ banques, Email...)

Les prix internationaux

Nobel (1833-1896) Fields (1863-1932) Turing (1912-1954)

- Prix Nobel

riche car découvrit dynamite
pas de Nobel en maths car cocu?

- Médaille Fields (maths)

interdit aux matheux de plus de 40 ans!

- Prix Turing (info)

inventa un ordinateur (machine de Turing)
Turing suicidé avec pomme au cyanure

Grandes conjectures XXI^e siècle :

Fermat ($a^n + b^n = c^n$) (démontré Wiles 1995)
P=NP?
Hypothèse de Riemann sur fonction zêta

Prospective

Grandes avancées de l'humanité :
alphabet, démocratie, mathématique, philosophie, lois, imprimerie

Prochain millénaire :
génie génétique (bionique)

Futur en maths-info :

- Informatique théorique :
  automatisation de calculs
  preuve automatique
  sécurité des programmes

- Informatique pratique :
  machines plus rapides (limitations)
  (miniaturisation, autres technologies, photon, quantique)
  ergonomie

	Université		Classes préparatoires	IUP; Écoles d'ingénieurs	IUT
bac+1	DEUG 1		Maths sup	1	1
bac+2	DEUG 2		Math spé	2	2 (DUT)
bac+3	Licence		1	3	
bac+4	maîtrise	IUFM1	2	4	
bac+5	DEA ou DESS	IUFM2	3	5	
bac+6 à +8	thèse				

Points de branchements :

• Université → Écoles :

après un DEUG : école d'ingénieur OK

après licence : grande école OK

• Écoles → Université :

aprés prépa, DUT : DEUG ou licence OK

• Ingénieur → Recherche

après diplôme d'ingénieur, DEA OK

La voie à suivre :

• Enseignement (primaire/secondaire) :

IUFM (Capes) (maîtrise pour agrégation)

• Enseignement (université) : thèse (doctorat)

• Recherche (université) : thèse (doctorat)

• Recherche (entreprise) : grandes écoles, DESS, thèse

• Ingénieur : grandes écoles, école d'ingénieur, IUP, DESS, IUT

Quelques instituts de recherche :
CEA (physique atomique)
CERN (physique nucléaire)
CNRS (pluridisciplinaire)
DGA (militaire)
IGN (géographie) IHESS (sciences sociales)
INRA (agronomie)
INREPS (sports)
INRETS (transports)
INRIA (informatique)
INSEE (statistique)
INSERM (médecine)

Vulgarisation

- *Émissions télé*

"*Archimède*" les mardis 19h-19h45 sur Arte
"*Pi=3.14*" les samedis 15h30 sur La Cinquième
"*E=M6*" les dimanches à 20h sur M6

- *Revues*

sciences : Pour la Science, La Recherche
maths : Tangente, Quadrature

- *Livres*

A. Dahan-Dalmedico & J.Peiffer : "Une Histoire des Mathématiques" Point Seuil
J.P Delahaye : "Logique, informatique et paradoxes", Belin
J.P Delahaye : "Le fascinant nombre pi", Belin

- *Sites internet*

Histoire des maths (St-Andrews) :
http://www-groups.dcs.st-and.ac.uk/~history/
Informatique : http://www.inria.fr/