UNE HISTOIRE DES MATHEMATIQUES

JEAN CAILLIEZ

SOMMAIRE

Nombres constructibles

Nombres algébriques

Un nombre *a* (réel ou complexe) est dit *algébrique* s'i l est racine d'un polynôme non nul à coefficients entiers

Exemples : nombres rationnels, *i* , $\sqrt{2}$ …

autres : **nombres transcendants**

nombre de Liouville (1844) : $\sum_{n>0} 10^{-n!}$

nombre *e* (Hermite 1873)

nombre π (Lindeman 1882)

Théorème de Gelfond –Schneider (1934) (7ème pb de Hilbert) *a* algébrique ($a \neq 0$ et $a \neq 1$) et *b* algébrique irrationnel alors a^b est transcendant (ex : $2^{\sqrt{2}}$)

Nombres constructibles (règle et compas)

Théorème de Wantzel (1837) : nombre obtenu par addition, soustraction, multiplication, division et par extraction de racine carrée (point constructible)

Conditions nécessaires (pour qu'un nombre soit constructible) :

1- algébrique

2- racine d'un polynôme de degré 2^n

applications

1- duplication du cube : $\sqrt[3]{2}$ racine de $X^3 - 2 = 0$

2- trisection de l'angle : $\cos(\theta/3)$ racine de $4X^3 - 3X - \cos(\theta) = 0$

3- quadrature du cercle : construire un carré de même aire qu'un cercle donné

impossible car π est transcendant

polygones réguliers constructibles (Gauss – Wantzel 1837)

un polygone régulier à n cotés est constructible si

$$n = 2^k p_1 p_2 \dots p_r \quad (p_i \text{ tous distincts})$$

Les p_i sont choisis parmi les nombres premiers de Fermat

Nombres de Fermat : $F(k) = 2^{f(k)} + 1$ où $f(k)=2^k$

F(0)=3, F(1)=5, F(2)=17, F(3)=257, F(4)=65537 …

Polygones constructibles :

n= 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24 …

Equations polynomiales

équation du second degré : $ax^2 + bx + c = 0$ (a non nul)

$$x_{\pm} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

équation du 3ème degré : $x^3 + ax + b = 0$ (Cardan-Tartaglia 1545)

$\Delta = b^2 + 4/27\ a^3$

$$x = \sqrt[3]{\frac{-b + \sqrt{\Delta}}{2}} + \sqrt[3]{\frac{-b - \sqrt{\Delta}}{2}}$$

équation du 4ème degré (Ferrari 1555)

les équations de degré 2, 3, 4 sont résolubles par radicaux

et pour le 5ème degré ?

Niels Abel : pas de solution en terme de radicaux pour l'équation générale du 5ème degré (1824)

Evariste Galois a donné les conditions suffisantes pour déterminer les équations résolubles par radicaux (notion de groupe résoluble) (1829)

Associer à tout polynôme un groupe (groupe de Galois)

Exemple : $X^5 – 3X -1 = 0$ n'est pas résoluble par radicaux

Conjecture de Fermat

$$x^n + y^n = z^n$$

n'admet pas de solutions entières non nulles dès que n>2

conjecture émise par **Fermat** (1647)

résolue par **A. Wiles** (1995)

Cas n=2 : triplets pythagoriciens

$$x=a^2 - b^2 \text{ , } y=2ab \text{ , } z=a^2 + b^2 \quad (a>b)$$

démonstrations directes pour n=3, 4, 5 (Euler, Dirichlet …)

Analyse de Fourier

équation des cordes vibrantes

$$\begin{cases} \dfrac{\partial^2 u}{\partial t^2} = v^2 \dfrac{\partial^2 u}{\partial x^2} \\ u(x,0) = f(x) \quad f(0) = f(l) = 0 \end{cases}$$

Taylor (1715) : $u(x,t)=\sin(\pi x/l)\cos(\pi t v/l)$

Bernoulli (fin du 18ème siècle) solution par superposition des modes propres

$$u(x,t)=\sum_{n>0} b_n \sin(n\pi x/l)\cos(n\pi v t/l)$$

$$b_n = 1/l \int_{[o,l]} f(x)\sin(n\pi x/l)\,dx$$

Principe développé par Fourier (séries de Fourier début du 19ème siècle)
Si h est une fonction T-périodique :

$$h(x) \backsimeq \sum_n c_n(h) e^{2i\pi nx/T}$$

$$c_n(h) = 1/T \int_{[0,T]} h(t)\, e^{-2i\pi nt/T}\, dt$$

(coefficient de Fourier d'ordre n)

hypothèses de régularité sur la fonction h (Dirichlet 1829)

pour que h soit égal à sa série de Fourier

formule de Parseval (Plancherel)

$$\sum_n |c_n(h)|^2 = 1/T \int_{[0,T]} |h(x)|^2\, dx$$

séries trigonométriques (Cantor, Riemann …)

étude qui a atteint son apogée au milieu du 20ème siècle (Kahane, Katznelson, Carleson)

Transformée de Fourier et équation de la chaleur

$$\mathcal{F}f(x) = \int_{-\infty}^{+\infty} f(t)e^{-2i\pi tx}dt$$

$$f(t) = \int_{-\infty}^{+\infty} \mathcal{F}f(x)e^{2i\pi tx}\,dx$$

$$\begin{cases} \dfrac{\partial u}{\partial t} = a^2 \dfrac{\partial^2 u}{\partial x^2} \\ u(x,0) = f(x) \end{cases}$$

Généralisation

Extension au cas des groupes commutatifs

notion de caractère

théorème de Pontryagin

Extension au cas des groupes non commutatifs

représentation de groupe

exemples :

GL(n,R) (groupe des matrices inversibles)

O(n) (groupe orthogonal)

SO(1,3) (groupe de Lorentz)

Fonction zeta de Riemann

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$$

définie pour Re s>1

Formule d'Euler (1768)

$$\zeta(s) = \prod_{p \in P} \frac{1}{1 - p^{-s}}$$

zeta se prolonge analytiquement à C\{1}

les valeurs de ζ(2k) sont connues pour k entier

relation fonctionnelle

$$\zeta(s) = 2^s \pi^{s-1} \sin(\frac{\pi s}{2}) \Gamma(1-s) \zeta(1-s)$$

$$\Gamma(s) = \int_0^{+\infty} t^{s-1} e^{-t} dt$$

Zéros de la fonction zeta :

Zéros « triviaux » : s=-2, -4,…-2n,…

Zéros « non triviaux » : infinité dans la bande 0 < Re s <1

Conjecture de Riemann (1859) : les zéros sont situés sur la droite Re s=1/2

c'est le 8ème problème de Hilbert

conséquences importantes :

sur l'estimation de fonctions arithmétiques

sur la répartition des nombres premiers

sur la fonction $\pi(x)=\mathrm{Card}\{p\ ;\ p \text{ premier } p<x\}$

et pour quelques dollars de plus

Conjecture de Goldbach (1742) :

Tout nombre pair (>2) peut s'écrire comme la somme de deux nombres premiers (vérifiée jusque 2^{18})

Conjecture des nombres premiers jumeaux :

Les nombres premiers p et p+2 sont-ils en nombre infini ?

Conjecture de Syracuse (1952)

Si n pair ⇒ n/2 sinon ⇒ 3n+1 : au bout d'un nombre fini d'opérations on obtient 1 (vérifiée jusque 2^{62})

*** Conjecture de Poincaré** (Perelman 2003) ($2^{ème}$ pb Clay)

V variété compacte simplement connexe de dimension 3 sans bord est homéomorphe à la sphère de même dimension

n=4 Freedman 1982

n>4 Smale 1961

***Équations de Navier-Stokes** (6ème pb Clay)

$$\frac{\partial \rho}{\partial t} + \sum_{i=1}^{3} \frac{\partial}{\partial x_i}(\rho v_i) = 0$$

ρ masse volumique

v_i composantes du vecteur vitesse

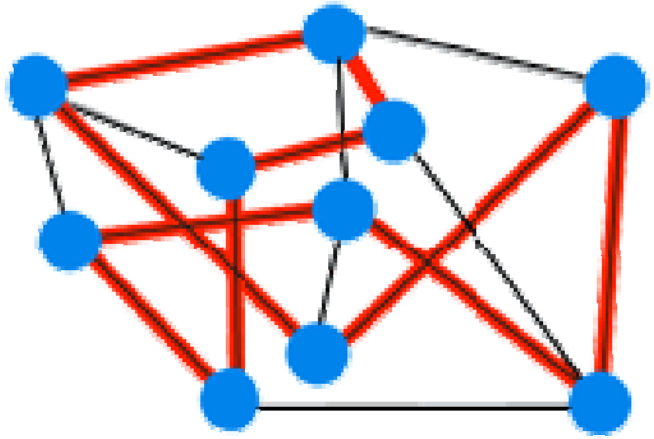
***Problème P≠NP ou P=NP ?** (4ème pb Clay)

sur la complexité des algorithmes

P =NP ??

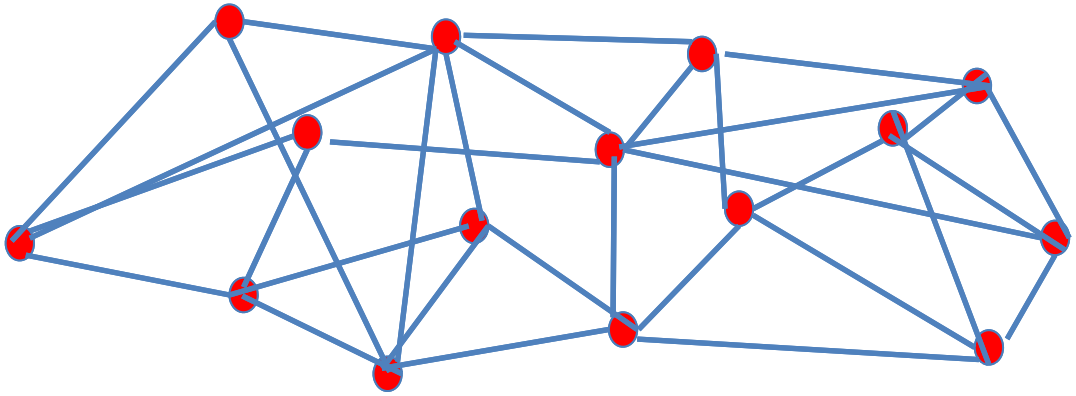
- Ou encore *“Tout ce que l'on peut vérifier facilement, peut-il être découvert aisément ? ”*.
- /ex Pb du Voyageur de commerce

  Visiter toute les villes d’un pays,une fois et une seule, et…revenir!!!
- Il est facile de *vérifier* qu’un chemin dans un graphe a cette propriété *On dit que c’est un circuit hamiltonien*

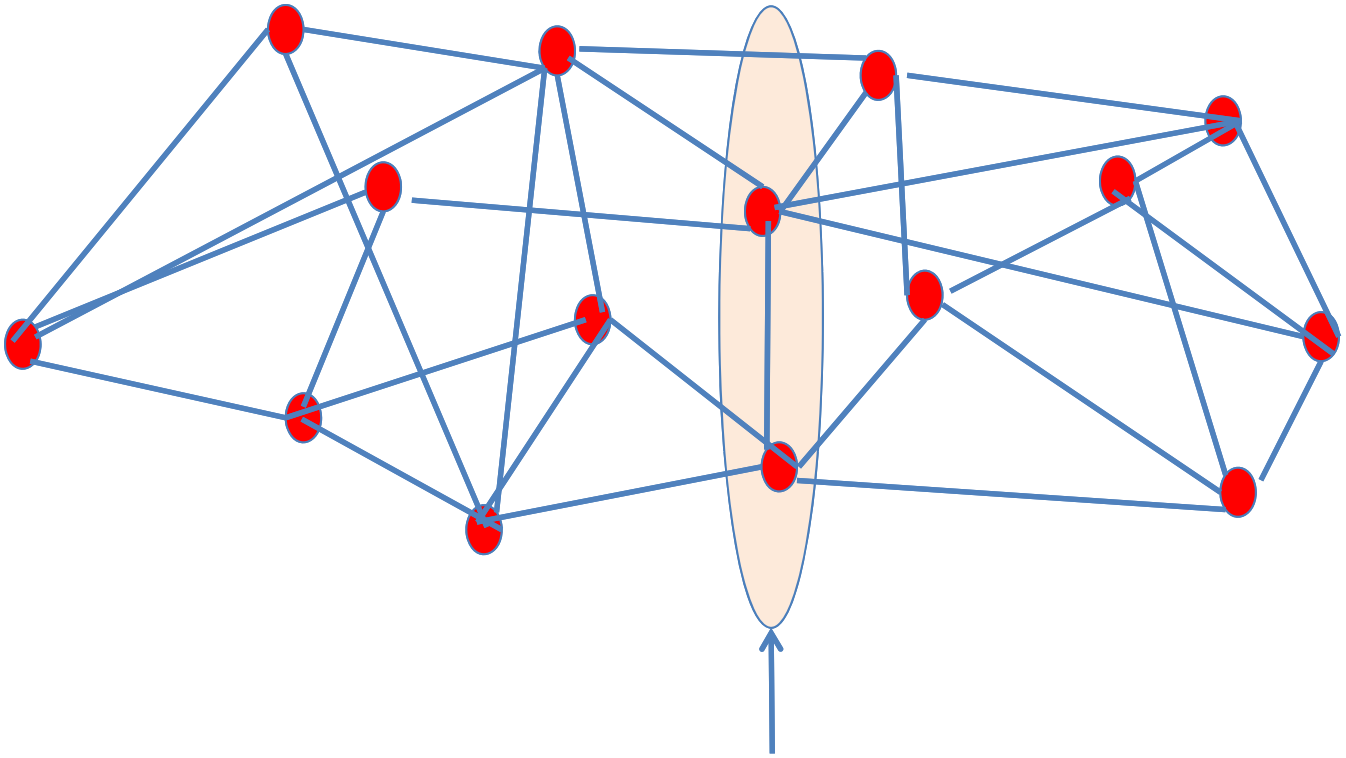


Tous les points ont deux et seulement deux arcs adjacents

Trouvez un circuit hamiltonien dans un graphe donné

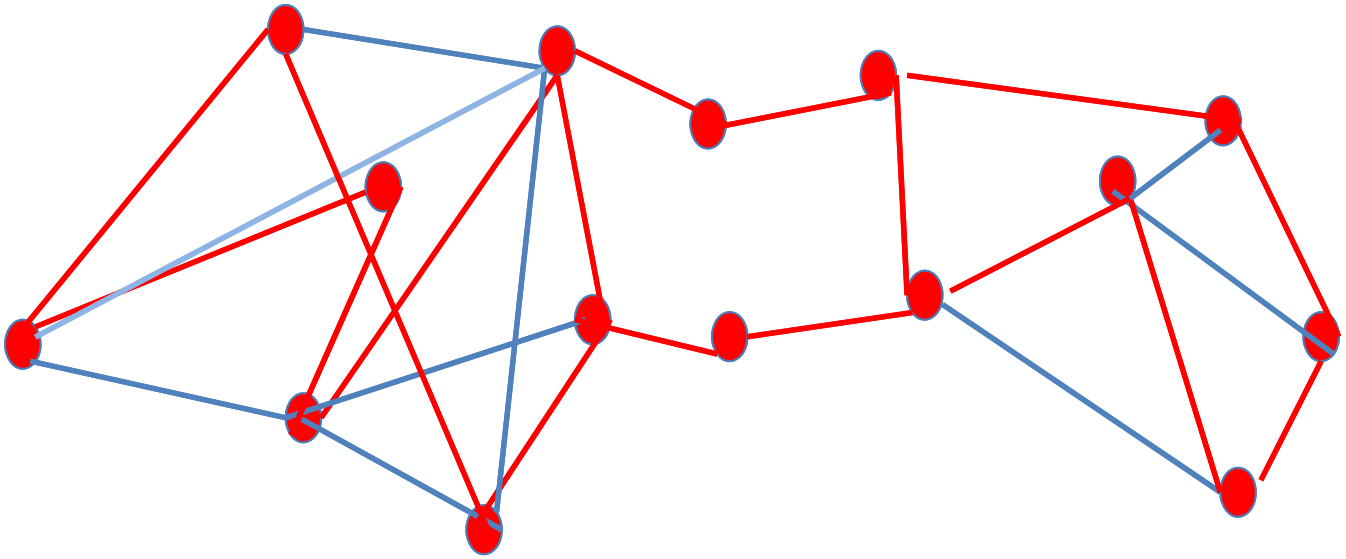


Hum!



Supprimons ces deux points

C’est un peu plus facile



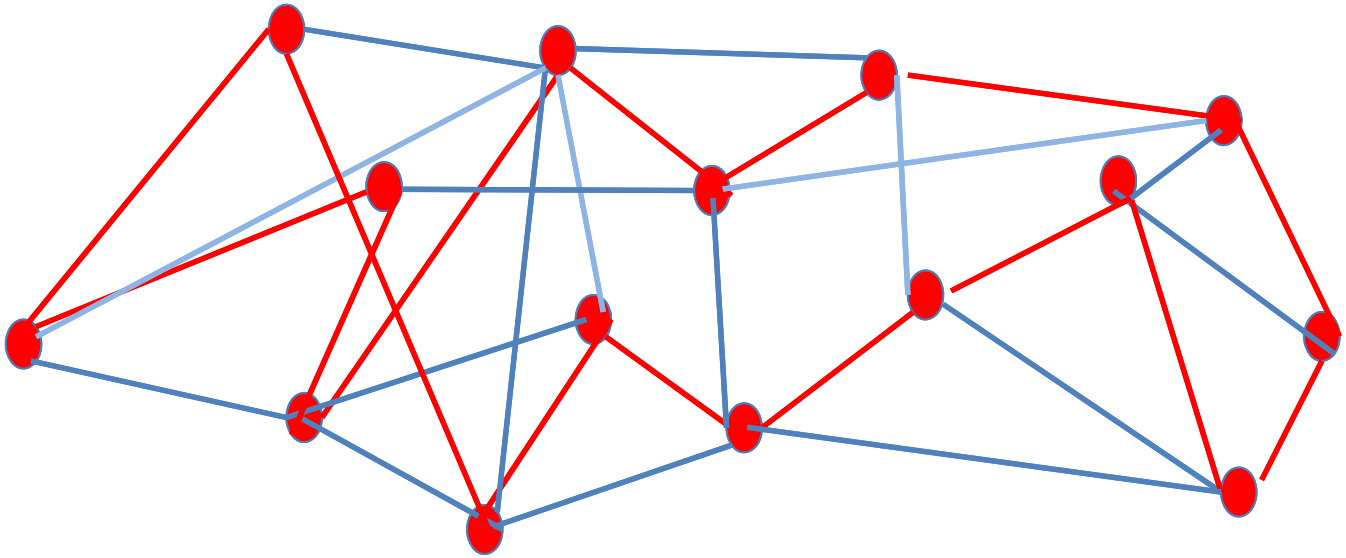
Alors remettons les points

ET REMETTONS-EN DEUX
POUR CHAQUE POINT

SUPPRIMONS DEUX ARCS

Et si on revient au graphe initial

ON A TROUVÉ!!



On a eu de la chance!! ….: cas particulier + construit pour cela

- En général trouver un chemin hamiltonien dans un graphe donné n’est pas facile:
- aujourd'hui, aucun algorithme efficace ne le permet. En revanche, si P = NP, savoir s'il existe des chemins hamiltoniens sera facile.

P =NP ??

C’est un problème de calculabilité en informatique théorique

Hilbert,Turing

- Une fonction ***f*** es**t calculable** si *f(x)* est calculable en un temps fini.
- Il existe de nombreuses fonctions non calculables, en particulier en théorie des ensembles.
- Il est donc fondamental de savoir si une fonction est calculable **avant** de programmer un algorithme qui bouclerait infiniment!!!
- */ex Dire a priori si un algorithme va s’arrêter ou non **est incalculable***

Plus finement

- **Un problème de décision est de la classe P** s'il peut être décidé sur une machine de Turing déterministe en temps polynomial par rapport à la taille de l'entrée
  - /ex Le problème de savoir si un entier est premier ou non peut-être résolu par un algorithme polynomial, donc de la classe P.
- **Un problème de décision D est P-complet s'il est dans P et** si tout problème de la classe P peut être réduit à D.
- */ex L'évaluation de circuit est P-complet: étant donnés un circuit booléen et une entrée, décider ce que va fournir le circuit en sortie*
- Relativement facile ➔ tout problème de P est "facile"!

NP Np-complet

- un **problème** de décision est dit **:**
- **NP** si:
  - Il est possible de **vérifier** une solution efficacement (en temps polynomial)
- **NP-complet**
  - s'il est **complet** et si tous les problèmes de la classe NP se ramènent à celui-ci via une réduction polynomiale
- *~ à il est au moins aussi difficile que tous les autres problèmes de NP*

- La question « P = NP ? ou P≠NP » n'est pas résolue
- Trouver un algorithme polynomial pour un problème NP-complet ou prouver qu'il n'en existe pas permettrait de savoir si P = NP ou P ≠ NP
- Trouver un chemin hamiltonien est NP-Complet
- Si P=NP alors cela pourrait se ramener un un problème NP complet

  donc à un problème P-complet

  donc à un problème *"facile"*

Espérons !

- Il semble aussi être le seul dont la résolution aurait des conséquences pratiques (il est lié à des centaines d'énoncés concrets) et sa portée philosophique est la plus grande :
- *la question « P = NP ? » concerne la nature de la recherche de solution(s) dans un ensemble exponentiel de possibilités, ce qui est le problème même de la recherche scientifique.*
- La question « P = NP ? » signifie à peu près : *« Ce que nous pouvons trouver rapidement lorsque nous avons de la chance, peut-il être trouvé aussi vite par un calcul intelligent ? ». Très sommairement, « l'intelligence peut-elle remplacer la chance ? »*

Références

- Alan Turing, « On Computable Numbers, with an Application to the Entscheidungsproblem », *Proc. London Math. Soc., 2e série, vol. 42, 1937, p. 230-265*
- **Jean Paul Delahaye P = NP, un problème à un million de dollars** *Pour la Science , n°334, en août 2005.*
- **Jean Gabriel Ganasca "Alan Turing : du calculable à l'indécidable"**

  http://interstices.info/jcms/c_5723/alan-turing-du-calculable-a-lindecidable

Distinctions

Médaille Fields

décernée à au plus quatre mathématiciens de moins de 40 ans à l'issue du Congrès International des Mathématiciens qui a lieu tous les 4 ans

1936 Ahlfors – Douglas

1950 Schwartz – Selberg

……

2010 Villani- Ngô Bao Châu …

Prix Abel

décerné par l'Académie des Sciences de Norvège

créé en 2003

2003 J.P. Serre

……

2008 J.Tits

2009 Gromov

L’HISTOIRE
n’est pas terminée