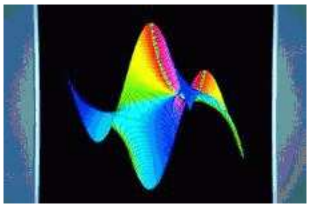
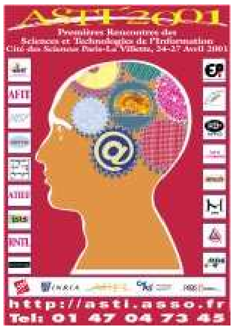



Informatique et Mathématiques

Philippe Flajolet, INRIA

25 avril 2001

L'informatique vue comme **science** du calcul

($\neq$ *technologie*)

- Comment *effectuer*? $\simeq$ aspects algorithmiques
- Comment *exprimer*? $\simeq$ aspects logico-sémantiques
- Comment *gérer*? aspects "systémiques"

Le Modem vu d'en dessous

Sciences . . . physiques et mathématiques: electricité, electronique, traitement de signal. Sans calcul differentiel et integral, EDP, analyse, point de modem!

Chip: logique booléenne,
BDD = logique booléenne + graphes + arbres
"automates finis & graphes de comportement"
(automatisme+informatique+linguistique formelle+logique+structures de données)
Optimisation combinatoire (placement), etc.

Fonctions: . . . Compression = Huffman dynamique

CACM 1958, vol. 1 (!)

Le Modem (II): ce qui transite

• JPEG, GIF, GZip, etc. Transf. de Fourier, compression Huffman, dictionnaires dynamiques (Lempel-Ziv)
Capitalise sur les structures de données liées aux arbres; optimisation fine en moyenne et/ou en probabilité.

• Accès Google, Altavista: de gigantesques usines algorithmiques sur les mots— accès rapide multidimensionnel, approché, etc.
Capitalise sur la combinatoire et l'algorithmique des mots, la théorie des automates, les probabilités discrètes

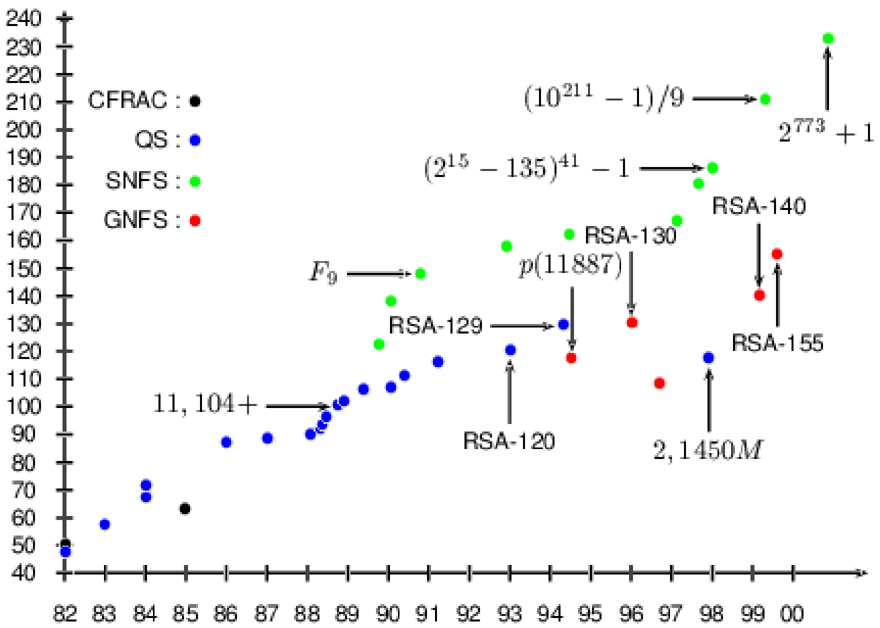
Le Modem (III)

• Cryptographie publique RSA

Capitalise sur groupes et corps finis; attaques par théorie des nombres très sophistiquée = algorithmique "randomisée" et structures arithmiques.

Émergence de systèmes de plus haute sécurité fondés sur les courbes elliptiques

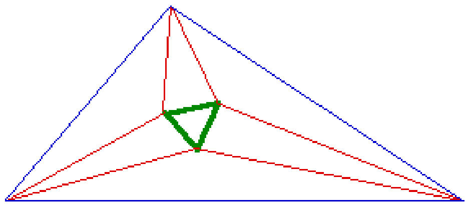
• Le mythe de la loi de Moore?

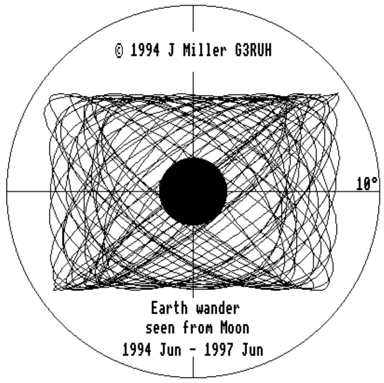


Morain, LIX; communauté CRYPTO en France !

$$e^{n} \quad \mapsto \quad e^{\sqrt{n}} \quad \mapsto \quad e^{\sqrt[3]{n}}$$

NB: RSA - (Hardy) = 1977 - 1947





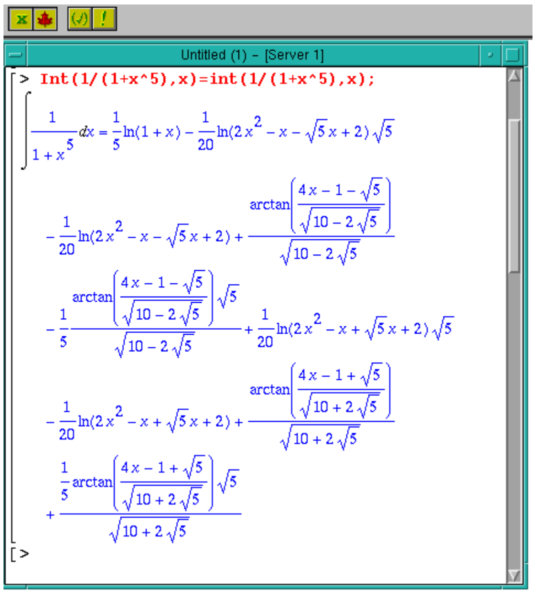
Instantanés: Le calcul formel

Delaunay 1867 (20 ans)

REDUCE 1970 (20 heures)

2001 ($\pm$ Immédiat)

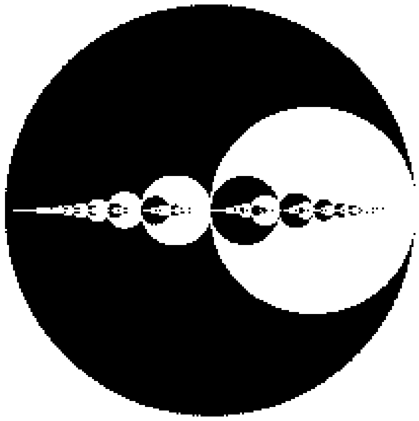
Structures de données, algorithmisation des mathématiques



$\Longrightarrow$ Renouveau "fonction spéciales" (Zeilberger, USA)

Experimental Mathematics (CECM, Vancouver)

+ Riche communauté MATHINFO/CALSYSF en France!



Instantanés
Géometrie: le zigzag discret-continu

Géométrie en vision, images (geom. class., diff., fractale)

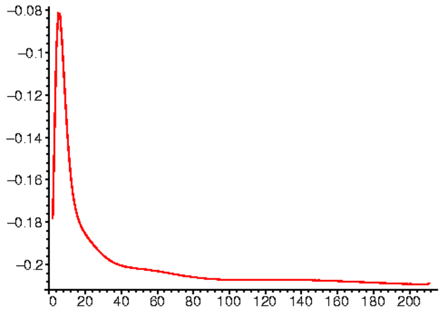
Géométrie discrète: robustesse/cohérence CAO

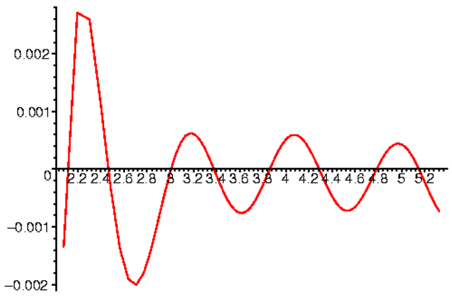
L'exemple de HAKMEM (Gosper 1973, Boissonnat 1997)

```
x ?  y => CF(x) ?  CF(y)
```

Analyse du tri associé & Riemann [Vallée, Clément, F.]

$$S(n) \simeq K_0 n \log n + K_1 n + Q(n) + K_2$$
$$K_0 = \frac{6 \log 2}{\pi^2}, \qquad K_1 = 18 \frac{\gamma \log 2}{\pi^2} + 9 \frac{(\log 2)^2}{\pi^2} - 72 \frac{\log 2 \zeta'(2)}{\pi^4} - \frac{1}{2}.$$

$Q(n)$: 



Instantanés
Des protocoles aux processus combinatoires

ALOHA $\mapsto$ ETHERNET $\mapsto$ Protocole en arbre

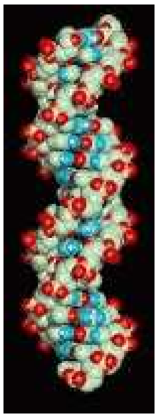
Analyse combinatoire
Transf. Mellin
Equations fonctionnelles, &c.

Optimisation: TV cable (cf trafic routier), IEEE 802.14

$\rightsquigarrow$ Calcul de Processus Combinatoires

♡ Gestion de gros dictionnaires. Quel est le vocabulaire de Balzac?

Communauté **ALÉA discret** en France (PROBA/INFO)



Instantanés: Mots & Séquences

Convergences!

Réseaux de neurones, linguistique formelle, automatismes

Automate finis

Analyse lexicale/syntaxique

Algorithmique des mots/textes

Quantification probabiliste

Analyse statistique des sequences

cf. BIOINFO, mots à Marne-la-Vallé, &c.

Informatique = Une démarche scientifique propre: monde inventé ($\neq$physique); e.g., objets dynamiques ou distribués information partielle &c ($\not\subseteq$ mathématiques);

Thèse de Knuth: "Tout en mathématique sert (ou servira un jour) en informatique".
cf. E. Wigner (1963): "The unreasonable effectiveness"
$\neq$ Hardy: useless $\Longrightarrow$ harmless, 1977-1947...
♡ Appl. inattendues, science non-planifiée, mais *viviers*

Informatique = Une science parmi les sciences.

Changements de perspective: notion d'effectivité
Complexité
Révision de pans des math. classiques (e.g., crypto, ϑ nombres)
Mathématiques discrètes $\in$ MATHINFO
Mathématiques expérimentales (**non**-disparition de la preuve!) $\in$ MATHINFO

L'oubli (occasionnel?) de la technologie pour la science?

Organisation de la communauté **MATHINFO** (PRC†)?