

Interacción entre Matemáticas e Informática

Un Viaje de Ida y Vuelta

Comisión de Informática de la R.S.M.E.

Jornadas Científicas de Informática y Matemática

Logroño, 29 de octubre de 2005



Sobre las Aplicaciones de la Matemática

Grosso modo se suele admitir la ecuación

$$\text{Matemáticas} = \text{Geometría} + \text{Álgebra} + \text{Análisis}$$

Las primeras aplicaciones estuvieron basadas en el Análisis:

- Creado por el afán de comprender ciertos fenómenos naturales
- La mayoría de las aplicaciones tenían que ver con el estudio de las fuerzas y su interacción con el entorno

Lema (histórico)

Las aplicaciones de la Matemática estaban basadas en la obtención y la explotación de la energía existente en la naturaleza



Sobre las Aplicaciones de la Matemática

No supone ninguna paradoja decir que en nuestras cábalas más teóricas podemos estar acercándonos lo más posible a las aplicaciones más prácticas.

A.N. Whitehead

No hay ninguna rama de la matemática, por abstracta que sea, que no pueda aplicarse algún día a los fenómenos del mundo real.

N.I. Lobachevsky



La Segunda Revolución Industrial

Durante el siglo XX se hizo patente *una nueva revolución industrial*, en la que **el concepto fundamental es la información**.

Su estudio, generación, almacenamiento, utilización e intercambio, necesita de sólidos fundamentos formales que la Matemática puede y debe proporcionar.

Lema (actualizado)

Las nuevas aplicaciones de la Matemática están basadas en la obtención y la explotación de la información



Matemáticas e Informática

La interacción entre las distintas áreas de las matemáticas entre sí, *así como con los ordenadores*, propicia el desarrollo de nuevas disciplinas, de interés tanto teórico como práctico:

Cálculo Simbólico	Lógica Computacional
Geometría Computacional	Lógica Algebraica
Álgebra Computacional	Lógica Geométrica
⋮	⋮



Las Matemáticas según la R.A.E.

- No se incluye en el Diccionario de Autoridades
- *Ciencia, que trata de la cantidad en quanto mensurable; cuyos principales fundamentos son la geometría y aritmética (ed. 1780)*
- *Ciencia, que trata de la cantidad en quanto mensurable (ed. 1803)*
- *Ciencia que trata de la cantidad (ed. 1832)*
- *Ciencia deductiva que estudia las propiedades de los entes abstractos, como números, figuras geométricas o símbolos, y sus relaciones (ed. 2001)*

Desde la edición de 1899 se incluyen las siguientes distinciones:

- [— Pura:] *Estudio de la cantidad considerada en abstracto.*
- [— Aplicada:] *Estudio de la cantidad considerada en relación con ciertos fenómenos físicos.*



Algunos Hitos

Galardonados con el premio Turing (1968–1990)

- R. Hamming [T'68]. Métodos numéricos, códigos autocorrectores
- Wilkinson [T'70]. Análisis numérico. Computación en Álgebra Lineal
- E. Dijkstra [T'72]. Teoría de grafos. ALGOL
- D. Knuth [T'74]. Teoría de algoritmos.
- S. Cook [T'82]. Teoría de la complejidad
- R. Karp [T'85]. Teoría de NP-completitud
- W. Kahan [T'86]. Análisis numérico. Computación con coma flotante
- R. Tarjan [T'86,N'82]. Aspectos matemáticos de la computación.



Algunos Hitos

Galardonados con el premio Turing (1990–2005)

- Robin Milner [T'91]. Lógica de funciones computables
- Stearns/Hartmanis [T'93]. Complejidad computacional
- Manuel Blum [T'95]. Complejidad computacional aplicada a la criptografía y a la verificación de programas
- Amir Pnuelli [T'96]. Lógica temporal para verificación
- Andrew C Yao [T'00]. Complejidad de la generación de números pseudo-aleatorios. Criptografía
- Rivest/Shamir/Adleman [T'02]. Algoritmo de encriptado RSA



Algunos Hitos

Galardonados con premios Gödel y premios Knuth

- Jerrum/Sinclair [G'96]. Cadenas de Markov y teoría de grafos
- P. Shor [G'99,N'98]. Algoritmo cuántico de factorización
- Herlihy&Shavit/Saks&Zaharoglou [G'02]. Uso de la topología de complejos simpliciales para la computación asíncrona
- Lovász [K'99]. Reducción de bases de retículos



Algunos Hitos

Galardonados con premios Herbrand

- L. Wos [H'92]. Deducción automática en problemas de álgebras de Boole, quasi-retículos, etc
- G. Huet [H'98]. Desarrollo del sistema semiautomático de demostración Coq
- Boyer/Moore [H'99]. Verificadores semi-automáticos NQTHM, ACL2
- W. McCune [H'00]. Ded. automática en álgebra abstracta y geometría algebraica



Algunos Hitos

Galardonados con premios Nevalinna

- R. Tarjan [N'82,T'86]. Aspectos matemáticos de la computación.
- L. Valiant [N'86]. Teoría de problemas de recuento
- A. Razborov [N'90]. Cotas inferiores de complejidad computacional. Combinatoria
- A. Wigderson [N'94]. Complejidad computacional, criptografía, computación cuántica
- P. Shor [N'98,G'99]. Algoritmo cuántico de factorización
- M. Sudan [N'02]. Caracterización probabilista de la clase NP



Temas de discusión

- Áreas matemáticas de interés para la informática
- Áreas de investigación informática que demandan matemática
- Informática y Matemática en las aulas
- ...

