Universidad Complutense de Madrid
Facultad de Ciencias Matemáticas
Departamento de Algebra
Teléfono: 91 394 45 70, Fax: 91 394 46 62
Correo electrónico: Algebra@mat.ucm.es

SEMINARIO DE GEOMETRÍA ALGEBRAICA

Martes 22 de abril de 2014, **13:00**, Seminario 238

Pedro Berrizbeitia

Universidad Simón Bolívar, Caracas, visitante en la UAM actualmente

Impartirá la conferencia

Sobre el estado actual de AKS

Resumen.
En esta charla empezaremos repasando las ideas principles del algoritmo AKS, llamado asíen honor a sus autores, Manindra Agrawal,Neeraj Kayal y Nitin Saxena, quienes en agosto de 2002 sorprendieron a la comunidad científica internacional con la presentación de este algoritmo "polinomial", que distingue a los números primos de los compuestos, poniendo fin a la cuestión de la existencia de un tal algoritmo.

Los autores de AKS pudieron probar el que número de operaciones que requiere el algoritmo para decidir si un número natural n es primo o compuesto, está acotado superiormente por un polinomio de grado $12+\epsilon$ en el $logn$, y mostraron que un tal polinomio no podía tener grado 6 o menor.

Pocos meses después, pude producir una variante del algoritmo AKS, el primero de una serie de resultados que más adelante fueron bautizados por Granville como la versión práctica de AKS. Para decirlo en dos palabras, la variante reemplaza el 6 por un 4.

El objetivo de la charla es explicar el resultado, junto con las ideas que me llevaron a él. Terminaré describiendo brevemente los resultados posteriores y comentando sobre la situación actual de AKS.