CONFERÈNCIA

Nudos, trenzas y criptografía

Dr. Juan González-Meneses

Departamento de Álgebra

Universidad de Sevilla

Resum

Desde sus orígenes, en los años 20, la principal aplicación de los grupos de trenzas ha sido la teoría de nudos. En la actualidad aún se espera resolver importantes problemas --por ejemplo, encontrar un algoritmo suficientemente rápido para distinguir nudos-- usando grupos de trenzas.

Pero en los últimos 6 años se ha descubierto una nueva y sorprendente aplicación de las trenzas: la criptografía. Curiosamente, la gran dificultad de los problemas que interesan en teoría de nudos hace que las trenzas sirvan para codificar información, mediante criptosistemas de clave pública. En esta charla describiremos la relación entre las trenzas y los nudos, qué problemas interesa resolver, cómo se pueden usar las trenzas para codificar datos, y cuál es la situación actual en estos temas.

Dimecres, 2 de març de 2005, a les 12h

Sala d'Actes de la

Facultat de Matemàtiques i Estadística

C. Pau Gargallo, 5 - Barcelona

Aquesta conferència, organitzada en col·laboració amb la Societat Catalana de Matemàtiques, serà repetida el dia 3 de març (dijous), a les 12.00 a la Sala de Graus de la Facultat de Ciències de la Universitat Autònoma de Barcelona

UNIVERSITAT POLITÈCNICA DE CATALUNYA