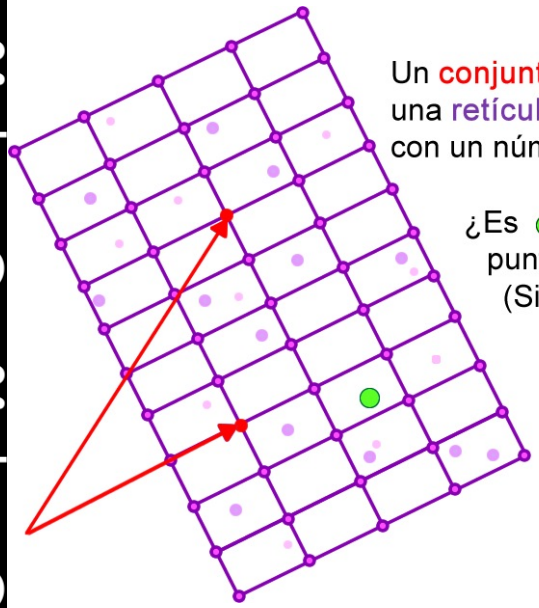
¿Todavía te causa ansiedad navegar por Internet?

COLOQUIO DE MATEMÁTICAS
Expositor: Andreu Boada de Atela
Martes 18 de febrero del 2014
Salón 102. De 2:30 a 3:30 p.m.



Un conjunto de vectores define una retícula multidimensional con un número infinito de puntos.

¿Es ● cercano a algún punto de la retícula? (Sin ver el dibujo.)

La criptografía es el estudio de técnicas, algoritmos y estrategias para comunicar información de tal forma que el adversario no conozca el contenido del mensaje que se va a enviar.

Los algoritmos criptográficos están diseñados bajo el supuesto de la dificultad computacional que se requiere para resolver algún problema determinado. Aún cuando en teoría sea posible que el adversario rompa dicho sistema, en la práctica no lo es.

La teoría de retículas tiene propiedades interesantes en criptografía. En esta plática se presentarán criptosistemas basados en problemas matemáticos difíciles de resolver computacionalmente, como el famoso problema de la mochila (*knapsack*) y el problema "aprendiendo con errores" (*LWE*), comunes en Investigación de Operaciones y Aprendizaje Estadístico, respectivamente. En estos sistemas la teoría de retículas juega un papel importantísimo en el análisis y diseño de estos algoritmos criptográficos.

Habrá pizzas y refrescos.