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

SEMINARIO DE GEOMETRÍA ALGEBRAICA

Jueves 18 de octubre de 2007, 13:00, Seminario 238

Enric Nart

Universidad Autónoma de Barcelona

Impartirá la conferencia

Función zeta y exponente criptográfico de curvas supersingulares de género 2 sobre cuerpos finitos

Resumen: El exponente criptográfico de una curva algebraica sobre un cuerpo finito es un invariante que mide la seguridad de la curva frente al ataque de Menezes-Okamoto-Vanstone, que reduce el problema del logaritmo discreto en su Jacobiana al problema del logaritmo discreto sobre el grupo multiplicativo de un cuerpo finito. Este invariante está determinado por la función zeta de la curva, de manera que su cálculo para una curva genérica pasa por los algoritmos standard de conteo de puntos de la curva. En la charla se mostrará un procedimento directo (no algorítmico) para calcular la función zeta (y por tanto el exponente criptográfico) de curvas supersingulares de género 2 con muchos automorfismos.