

# Seminario de Teoría de Números

Miércoles, 25 de enero de 2012

16:00 h. **Sala Naranja** (ICMat, Campus de Cantoblanco)

**Moubariz Garaev**

Universidad Nacional Autónoma de México

## Concentración de puntos sobre curvas elípticas en cuerpos primos

(trabajo conjunto con M.-C. Chang, J. Cilleruelo, J. Hernández,  
I. Shparlinski y A. Zumalacárregui)

### Abstract:

Sea  $F_p$  el cuerpo de las clases residuales módulo un primo  $p$  y sean  $J_1, J_2$  dos intervalos en  $F_p$  de longitud  $M$ . Para un polinomio cúbico  $f(x)$  en  $F_p[X]$ , consideramos la congruencia  $y^2 = f(x) \pmod{p}$  donde  $(x, y) \in J_1 \times J_2$ . En esta plática voy a hablar sobre nuevas cotas superiores para el número de soluciones de esta congruencia y explicaré las ideas principales de la demostración.

