Meeting: 1007, Santa Barbara, California, SS 3A, Special Session on Recent Advances in Combinatorial Number Theory

1007-11-119 **Jean Bourgain*** (bourgain@math.ias.edu), School of Math, Institute for Advanced Study, Princeton, NJ 08540. *Subgroup exponential sums in problems of pseudo-randomness and circuit complexity.*

Unconditional distributional properties for Diffie-Hellmann pairs and RSA generators are derived from a new Mordell type exponential sum.

It is shown that the correlation between parity and a degree d polynomial in n variables mod q (q fixed and odd,d fixed) is exponentially small in n. (Received February 14, 2005)