

1016-11-279

Tanja Lange* (t.lange@mat.dtu.dk), Department of Mathematics, Technical University of Denmark, Matematiktorvet 303, 2800 Kongens Lyngby, Denmark, and **Igor E. Shparlinski**.

Distribution of Some Sequences of Points on Elliptic Curves.

We estimate character sums over points on elliptic curves over a finite field \mathbb{F}_q of q elements. Pseudorandom sequences can be constructed by taking linear combinations with small coefficients (for example, from the set $\{-1, 0, 1\}$) of a fixed vector of points, which forms the seed of the generator. We consider several particular cases of this general approach which are of special practical interest and have occurred in the literature. For each of them we show that the resulting sequence has good uniformity of distribution properties. (Received February 14, 2006)