Certain Exponential Sums and Random Walks on Elliptic Curves

Tanja Lange and Igor E. Shparlinski

Abstract. For a given elliptic curve $E$, we obtain an upper bound on the discrepancy of sets of multiples $z_i G$ where $z_i$ runs through a sequence $Z = (z_1, \ldots, z_T)$ such that $k z_1, \ldots, k z_T$ is a permutation of $z_1, \ldots, z_T$, both sequences taken modulo $t$, for sufficiently many distinct values of $k$ modulo $t$.

We apply this result to studying an analogue of the power generator over an elliptic curve. These results are elliptic curve analogues of those obtained for multiplicative groups of finite fields and residue rings.