CORR 99-05

The Xedni Calculus and the Elliptic Curve Discrete Logarithm Problem

Joseph H. Silverman*

Abstract Let $E/\mathbb{F}_p$ be an elliptic curve defined over a finite field, and let S, $T \in E(\mathbb{F}_p)$ be two points on E. The *Elliptic Curve Discrete Logarithm Problem* (ECDLP) asks to find an integer m so that $S = mT$ in $E(\mathbb{F}_p)$. In this note we give a new algorithm, dubbed the Xedni Calculus, which might be used to solve the ECDLP. As remarked by Neal Koblitz, the Xedni method is also applicable to the classical discrete logarithm problem for $\mathbb{F}_p^*$ and to the integer factorization problem.